

SIEMENS

User Manual

SURPASS hiD 6610 S311 R1.0

UMN:CLI

A50010-Y3-B100-2-7619



Important Notice on Product Safety

Elevated voltages are inevitably present at specific points in this electrical equipment. Some of the parts may also have elevated operating temperatures.

Non-observance of these conditions and the safety instructions can result in personal injury or in property damage.

Therefore, only trained and qualified personnel may install and maintain the system.

The system complies with the standard EN 60950-1 / IEC 60950-1. All equipment connected has to comply with the applicable safety standards.

The same text in German:

Wichtiger Hinweis zur Produktsicherheit

In elektrischen Anlagen stehen zwangsläufig bestimmte Teile der Geräte unter Spannung. Einige Teile können auch eine hohe Betriebstemperatur aufweisen.

Eine Nichtbeachtung dieser Situation und der Warnungshinweise kann zu Körperverletzungen und Sachschäden führen.

Deshalb wird vorausgesetzt, dass nur geschultes und qualifiziertes Personal die Anlagen installiert und wartet.

Das System entspricht den Anforderungen der EN 60950-1 / IEC 60950-1. Angeschlossene Geräte müssen die zutreffenden Sicherheitsbestimmungen erfüllen.

Trademarks:

All designations used in this document can be trademarks, the use of which by third parties for their own purposes could violate the rights of their owners.

Copyright (C) Siemens AG 2005-2006.

Issued by the Communications Group
Hofmannstraße 51
D-81359 München

Technical modifications possible.
Technical specifications and features are binding only insofar as they are specifically and expressly agreed upon in a written contract.

Reason for Update

Summary: Updated for Issue 2

Details:

Chapter/Section	Reason for Update
All	Documentation template changed
5	Port Configuration updated
6.1.11.1	CPU Load added
6.1.11.4	System Temperature added
6.3.10	Statistics of CPU load added
7.1.8.2	SNMP trap mode added
7.6.2.1	Rule Creation updated
7.6.2.3	Packet Classification updated
7.10	Port Security added
7.13.3	ARP Inspection added
7.14.3	The Policy of Unreached Messages added
8.1.4	VLAN Description added
8.1.7.1	Port Isolation added
8.3.7	Root Guard added
8.3.9.5	BPDU Filter added
8.3.9.6	BPDU Guard added
8.8	Dynamic Host Configuration Protocol Updated
8.8.2.8	IP Address Assignment without CID added
8.8.5	DHCP Relay Agent added
8.8.6.5	DHCP Option82 Trust Packet added
8.8.6.6	Simplified DHCP option82 added
8.8.7	DHCP Client added
8.8.8	DHCP snooping added
8.8.12	Debugging DHCP added
9.2	PIM-SM updated

Issue History

Issue Number	Date of Issue	Reason for Update
01	02/2005	Initial release
02	04/2006	Updated for version 2

This document consists of a total of 310 pages. All pages are issue 2.

Contents

1	Introduction	19
1.1	Audience	19
1.2	Document Structure	19
1.3	Document Convention	20
1.4	Document Notation	20
1.5	CE Declaration of Conformity	20
1.6	GPL/LGPL Warranty and Liability Exclusion	21
2	System Overview	22
2.1	System Features	23
3	Command Line Interface (CLI)	25
3.1	Command Mode	25
3.1.1	Privileged EXEC View Mode	27
3.1.2	Privileged EXEC Enable Mode	27
3.1.3	Global Configuration Mode	27
3.1.4	Bridge Configuration Mode	28
3.1.5	Rule Configuration Mode	29
3.1.6	DHCP Configuration Mode	30
3.1.7	DHCP Option 82 Configuration Mode	30
3.1.8	Interface Configuration Mode	31
3.1.9	RMON Configuration Mode	31
3.1.10	PIM Configuration Mode	32
3.1.11	Router Configuration Mode	32
3.1.12	VRRP Configuration Mode	33
3.1.13	Route-Map Configuration Mode	33
3.2	Useful Tips	34
3.2.1	Listing Available Commands	34
3.2.2	Calling Command History	36
3.2.3	Using Abbreviation	36
3.2.4	Using Command of Privileged EXEC Enable Mode	37
3.2.5	Exit Current Command Mode	37
4	System Connection and IP Address	38
4.1	System Connection	38
4.1.1	System Login	38
4.1.2	Password for Privileged EXEC Mode	39
4.1.3	Changing Login Password	40
4.1.4	Management for System Account	40
4.1.4.1	Creating System Account	40
4.1.4.2	Configuring Security Level	41
4.1.5	Limiting Number of User	45
4.1.6	Telnet Access	45
4.1.7	Auto Log-out	46
4.1.8	System Rebooting	46
4.1.8.1	Manual System Rebooting	46
4.1.8.2	Auto System Rebooting	47
4.2	System Authentication	48

4.2.1	Authentication Method	48
4.2.2	Authentication Interface	48
4.2.3	Primary Authentication Method	48
4.2.4	RADIUS Server	49
4.2.4.1	RADIUS Server for System Authentication	49
4.2.4.2	RADIUS Server Priority	49
4.2.4.3	Timeout of Authentication Request	49
4.2.4.4	Frequency of Retransmit	49
4.2.5	TACACS Server	50
4.2.5.1	TACACS Server for System Authentication	50
4.2.5.2	TACACS Server Priority	50
4.2.5.3	Timeout of Authentication Request	50
4.2.5.4	Additional TACACS+ Configuration	50
4.2.6	Accounting Mode	51
4.2.7	Displaying System Authentication	51
4.3	Assigning IP Address	52
4.3.1	Enabling Interface	52
4.3.2	Disabling Interface	53
4.3.3	Assigning IP Address to Network Interface	53
4.3.4	Static Route and Default Gateway	54
4.3.5	Displaying Interface	55
4.4	SSH (Secure Shell)	56
4.4.1	SSH Server	56
4.4.1.1	Enabling SSH Server	56
4.4.1.2	Displaying On-line SSH Client	56
4.4.1.3	Disconnecting SSH Client	56
4.4.1.4	Displaying Connection History of SSH Client	56
4.4.2	SSH Client	57
4.4.2.1	Login to SSH Server	57
4.4.2.2	File Copy	57
4.4.2.3	Getting access to FTP	57
4.4.2.4	Configuring Authentication Key	57
4.5	802.1x Authentication	59
4.5.1	802.1x Authentication	60
4.5.1.1	Enabling 802.1x	60
4.5.1.2	Configuring RADIUS Server	60
4.5.1.3	Configuring Authentication Mode	61
4.5.1.4	Authentication Port	62
4.5.1.5	Force Authorization	62
4.5.1.6	Configuring Interval for Retransmitting Request/Identity Packet	62
4.5.1.7	Configuring Number of Request to RADIUS Server	63
4.5.1.8	Configuring Interval of Request to RADIUS Server	63
4.5.2	802.1x Re-Authentication	63
4.5.2.1	Enabling 802.1x Re-Authentication	64
4.5.2.2	Configuring the Interval of Re-Authentication	64
4.5.2.3	Configuring the Interval of Requesting Re-authentication	64
4.5.2.4	802.1x Re-authentication	65
4.5.3	Initializing Authentication Status	65
4.5.4	Applying Default Value	65
4.5.5	Displaying 802.1x Configuration	65
4.5.6	802.1x User Authentication Statistic	65

4.5.7	Sample Configuration	66
5	Port Configuration.....	68
5.1	Port Basic	68
5.2	Ethernet Port Configuration	69
5.2.1	Enabling Ethernet Port	69
5.2.2	Auto-negotiation	69
5.2.3	Transmit Rate	70
5.2.4	Duplex Mode	70
5.2.5	Flow Control	71
5.2.6	Port Description	72
5.2.7	Traffic Statistics.....	72
5.2.8	Port Status	73
5.3	Port Mirroring.....	73
6	System Environment	76
6.1	Environment Configuration.....	76
6.1.1	Host Name.....	76
6.1.2	Time and Date	76
6.1.3	Time Zone.....	77
6.1.4	Network Time Protocol	77
6.1.5	Simple Network Time Protocol (SNTP)	78
6.1.6	Terminal Configuration.....	79
6.1.7	Login Banner	79
6.1.8	DNS Server	79
6.1.9	Fan Operation.....	80
6.1.10	Disabling Daemon Operation	80
6.1.11	System Threshold.....	81
6.1.11.1	CPU Load	81
6.1.11.2	Port Traffic	81
6.1.11.3	Fan Operation.....	82
6.1.11.4	System Temperature	82
6.1.11.5	System Memory.....	82
6.2	Configuration Management	83
6.2.1	Displaying System Configuration	83
6.2.2	Saving System Configuration	83
6.2.3	Auto-Saving	84
6.2.4	System Configuration File	84
6.2.5	Restoring Default Configuration	85
6.3	System Management.....	86
6.3.1	Network Connection	86
6.3.2	IP ICMP Source-Routing	88
6.3.3	Tracing Packet Route	90
6.3.4	Displaying User Connecting to System	90
6.3.5	MAC Table	91
6.3.6	Running Time of System	91
6.3.7	System Information.....	92
6.3.8	System Memory Information	92
6.3.9	Average of CPU Load.....	92
6.3.10	Statistics of CPU Load.....	93
6.3.11	Running Process	94
6.3.12	Displaying System Image	94

6.3.13	Displaying Installed OS.....	95
6.3.14	Default OS	95
6.3.15	Switch Status	95
6.3.16	Tech Support.....	95
7	Network Management	96
7.1	Simple Network Management Protocol (SNMP)	96
7.1.1	SNMP Community	96
7.1.2	Information of SNMP Agent	97
7.1.3	SNMP Com2sec	98
7.1.4	SNMP Group	98
7.1.5	SNMP View Record	99
7.1.6	Permission to Access SNMP View Record.....	99
7.1.7	SNMP Version 3 User.....	100
7.1.8	SNMP Trap	100
7.1.8.1	SNMP Trap Host.....	101
7.1.8.2	SNMP Trap Mode	101
7.1.8.3	Enabling SNMP Trap	102
7.1.8.4	Disabling SNMP Trap	103
7.1.8.5	Displaying SNMP Trap.....	104
7.1.9	SNMP Alarm	105
7.1.9.1	Enabling Alarm Notification.....	105
7.1.9.2	Default Alarm Severity	105
7.1.9.3	Alarm Severity Criterion.....	105
7.1.9.4	Generic Alarm Severity.....	105
7.1.9.5	ADVA Alarm Severity	107
7.1.9.6	ERP Alarm Severity	108
7.1.9.7	STP Guard Alarm Severity.....	109
7.1.10	Displaying SNMP Configuration	109
7.1.11	Disabling SNMP.....	110
7.2	Operation, Administration and Maintenance (OAM).....	111
7.2.1	OAM Loopback	111
7.2.2	Local OAM Mode	112
7.2.3	OAM Unidirection.....	112
7.2.4	Remote OAM	112
7.2.5	Displaying OAM Configuration	113
7.3	Link Layer Discovery Protocol (LLDP).....	115
7.3.1	LLDP Operation	115
7.3.2	Enabling LLDP.....	115
7.3.3	LLDP Operation Type	115
7.3.4	Basic TLV	116
7.3.5	LLDP Message	116
7.3.6	Interval and Delay Time	116
7.3.7	Displaying LLDP Configuration.....	117
7.4	Remote Monitoring (RMON).....	118
7.4.1	RMON History.....	118
7.4.1.1	Source Port of Statistical Data	119
7.4.1.2	Subject of RMON History	119
7.4.1.3	Number of Sample Data	119
7.4.1.4	Interval of Sample Inquiry.....	120
7.4.1.5	Activating RMON History.....	120

7.4.1.6	Deleting Configuration of RMON History.....	120
7.4.1.7	Displaying RMON History.....	120
7.4.2	RMON Alarm	121
7.4.2.1	Subject of RMON Alarm	122
7.4.2.2	Object of Sample Inquiry	122
7.4.2.3	Absolute Comparison and Delta Comparison	122
7.4.2.4	Upper Bound of Threshold	122
7.4.2.5	Lower Bound of Threshold	123
7.4.2.6	Configuring Standard of the First Alarm	123
7.4.2.7	Interval of Sample Inquiry.....	124
7.4.2.8	Activating RMON Alarm.....	124
7.4.2.9	Deleting Configuration of RMON Alarm.....	124
7.4.2.10	Displaying RMON Alarm.....	124
7.4.3	RMON Event	125
7.4.3.1	Event Community	125
7.4.3.2	Event Description	125
7.4.3.3	Subject of RMON Event	125
7.4.3.4	Event Type.....	125
7.4.3.5	Activating RMON Event.....	126
7.4.3.6	Deleting Configuration of RMON Event.....	126
7.4.3.7	Displaying RMON Event.....	126
7.5	Syslog	127
7.5.1	Syslog Output Level	127
7.5.2	Facility Code.....	129
7.5.3	Syslog Bind Address.....	129
7.5.4	Debug Message for Remote Terminal.....	130
7.5.5	Enabling Syslog.....	130
7.5.6	Displaying Syslog Message	130
7.5.7	Displaying Syslog Configuration.....	130
7.6	Rule and QoS	131
7.6.1	How to Operate Rule and QoS.....	131
7.6.2	Rule Configuration.....	132
7.6.2.1	Rule Creation.....	132
7.6.2.2	Rule Priority	132
7.6.2.3	Packet Classification	133
7.6.2.4	Rule Action	135
7.6.2.5	Applying Rule	137
7.6.2.6	Modifying and Deleting Rule	137
7.6.2.7	Displaying Rule.....	137
7.6.3	QoS.....	139
7.6.3.1	Scheduling Algorithm.....	139
7.6.3.2	Qos Weight.....	142
7.6.3.3	Maximum and Minimum Bandwidth	142
7.6.3.4	Random Early Discard (RED)	143
7.6.3.5	Displaying QoS.....	143
7.6.4	Admin Access Rule.....	144
7.6.4.1	Rule Creation.....	144
7.6.4.2	Rule Priority	144
7.6.4.3	Packet Classification	145
7.6.4.4	Rule Action	146
7.6.4.5	Applying Rule	146

7.6.4.6	Modifying and Deleting Rule.....	147
7.6.4.7	Displaying Rule.....	147
7.7	NetBIOS Filtering.....	148
7.8	Martian Filtering.....	149
7.9	Max Host.....	150
7.9.1	Max New Hosts.....	151
7.10	Port Security	152
7.10.1	Port Security on Port.....	152
7.10.2	Port Security Aging	154
7.11	MAC Table	155
7.12	MAC Filtering.....	156
7.12.1	Default Policy of MAC Filtering.....	156
7.12.2	Adding Policy of MAC Filter.....	157
7.12.3	Deleting MAC Filter Policy.....	157
7.12.4	Listing of MAC Filter Policy.....	157
7.12.5	Displaying MAC Filter Policy	158
7.13	Address Resolution Protocol (ARP)	159
7.13.1	ARP Table	159
7.13.1.1	Registering ARP Table.....	159
7.13.1.2	Displaying ARP Table	160
7.13.2	ARP Alias.....	160
7.13.3	ARP-Inspection.....	161
7.13.3.1	Enabling ARP Inspection	161
7.13.3.2	ARP Inspection mapping policy.....	161
7.13.3.3	Configuring IP address-validation.....	162
7.13.3.4	Enabling match-mac.....	162
7.13.3.5	Displaying ARP Inspection	163
7.13.4	Gratuitous ARP	164
7.13.5	Proxy-ARP.....	164
7.14	ICMP Message Control.....	164
7.14.1	Blocking Echo Reply Message	165
7.14.2	Interval for Transmit ICMP Message	166
7.14.3	The policy of unreachable messages.....	167
7.15	IP TCP Flag Control.....	168
7.15.1	RST Configuration	168
7.15.2	SYN Configuration	168
7.16	Packet Dump	168
7.16.1	Verifying Packet Dump	169
7.16.1.1	Packet Dump by Protocol	169
7.16.1.2	Packet Dump with Option	169
7.16.2	Debug Packet Dump	171
8	System Main Functions	172
8.1	VLAN	172
8.1.1	Port-Based VLAN	173
8.1.1.1	Creating VLAN.....	174
8.1.1.2	Specifying PVID.....	174
8.1.1.3	Assigning Port to VLAN	174
8.1.1.4	Deleting VLAN	174
8.1.1.5	Displaying VLAN.....	175
8.1.2	Protocol-Based VLAN.....	175

8.1.3	Tagged VLAN	175
8.1.4	VLAN Description	176
8.1.5	Displaying VLAN Information	177
8.1.6	QinQ	177
8.1.6.1	Double Tagging Operation.....	178
8.1.6.2	Double Tagging Configuration	179
8.1.6.3	TPID Configuration	179
8.1.7	Layer 2 Isolation	180
8.1.7.1	Port Isolation.....	180
8.1.7.2	Shared VLAN.....	181
8.1.8	VLAN Translation.....	182
8.1.9	Sample Configuration	183
8.2	Link Aggregation.....	187
8.2.1	Port Trunk	187
8.2.1.1	Configuring Port Trunk.....	187
8.2.1.2	Disabling Port Trunk	188
8.2.1.3	Displaying Port Trunk Configuration.....	188
8.2.2	Link Aggregation Control Protocol (LACP)	189
8.2.2.1	Configuring LACP	189
8.2.2.2	Packet Route	190
8.2.2.3	Operating Mode of Member Port.....	190
8.2.2.4	Identifying Member Ports within LACP	191
8.2.2.5	BPDU Transmission Rate.....	191
8.2.2.6	Key value of Member Port.....	192
8.2.2.7	Priority of Member Port.....	192
8.2.2.8	Priority of Switch.....	192
8.2.2.9	Displaying LACP Configuration	193
8.3	Spanning-Tree Protocol (STP)	194
8.3.1	STP Operation	195
8.3.2	RSTP Operation	199
8.3.3	MSTP Operation	203
8.3.4	Configuring STP/RSTP/MSTP/PVSTP/PVRSTP Mode (Required).....	205
8.3.5	Configuring STP/RSTP/MSTP	206
8.3.5.1	Activating STP/RSTP/MSTP	206
8.3.5.2	Root Switch	206
8.3.5.3	Path-cost	206
8.3.5.4	Port-priority	207
8.3.5.5	MST Region.....	208
8.3.5.6	MSTP Protocol	209
8.3.5.7	Point-to-point MAC Parameters	209
8.3.5.8	Edge Ports.....	209
8.3.5.9	Displaying Configuration	210
8.3.6	Configuring PVSTP/PVRSTP	211
8.3.6.1	Activating PVSTP/PVRSTP.....	211
8.3.6.2	Root Switch	212
8.3.6.3	Path-cost	212
8.3.6.4	Port-priority	212
8.3.7	Root Guard.....	213
8.3.8	Restarting Protocol Migration	213
8.3.9	Bridge Protocol Data Unit Configuration	214
8.3.9.1	Hello Time.....	214

8.3.9.2	Forward Delay	215
8.3.9.3	Max Age	215
8.3.9.4	BPDU Hop	216
8.3.9.5	BPDU Filter	216
8.3.9.6	BPDU Guard	216
8.3.9.7	Self Loop Detection	217
8.3.9.8	Displaying BPDU Configuration	218
8.3.10	Sample Configuration	219
8.4	VRRP (Virtual Router Redundancy Protocol)	221
8.4.1	Configuring VRRP	222
8.4.1.1	Associated IP Address	222
8.4.1.2	Access to Associated IP Address	223
8.4.1.3	Master Router and Backup Router	223
8.4.1.4	VRRP Track Function	225
8.4.1.5	Authentication Password	226
8.4.1.6	Preempt	227
8.4.1.7	VRRP Statistics	228
8.5	Rate Limit	229
8.5.1	Configuring Rate Limit	229
8.5.2	Sample Configuration	229
8.6	Flood Guard	230
8.6.1	Configuring Flood-Guard	230
8.6.2	Sample Configuration	230
8.7	Bandwidth	231
8.8	Dynamic Host Configuration Protocol (DHCP)	232
8.8.1	DHCP Server	233
8.8.2	DHCP Pool	233
8.8.2.1	DHCP Pool Creation	233
8.8.2.2	DHCP Subnet	234
8.8.2.3	Subnet Default Gateway	234
8.8.2.4	IP Address Range	235
8.8.2.5	IP Lease Time	235
8.8.2.6	DNS Server	236
8.8.2.7	Manual Binding	236
8.8.2.8	Recognition of DHCP Client	236
8.8.2.9	Authorized ARP	236
8.8.2.10	Displaying Configuration	237
8.8.3	Registering Global DNS Server	238
8.8.4	Setting global lease Time	238
8.8.5	DHCP Relay Agent	239
8.8.5.1	Enable DHCP Relay Agent	239
8.8.5.2	Smart Relay Agent Forwarding	240
8.8.6	DHCP Option-82	240
8.8.6.1	Enabling DHCP Option-82	241
8.8.6.2	Option 82 Sub-Option	242
8.8.6.3	Option-82 Reforwarding Policy	242
8.8.6.4	Configuring option-82 information	243
8.8.6.5	Option-82 Trust Policy	246
8.8.6.6	Simplified DHCP Option 82 in Layer 2	247
8.8.7	DHCP Client	248
8.8.7.1	Enabling DHCP Client (Required)	248

8.8.7.2	DHCP Client ID.....	248
8.8.7.3	DHCP Class ID.....	248
8.8.7.4	Lease Time of Client.....	249
8.8.7.5	Forcing a Release or Renewal of DHCP Client.....	249
8.8.7.6	Displaying DHCP Client Configuration	249
8.8.8	DHCP Snooping	249
8.8.8.1	Enabling DHCP Snooping	250
8.8.8.2	DHCP snooping on port.....	250
8.8.8.3	DHCP Rate Limit on Layer 2	250
8.8.8.4	Displaying DHCP Snooping Configuration	250
8.8.9	Displaying DHCP Statistics and Configuration	251
8.8.10	Lease Database Back-up & Reset	251
8.8.11	DHCP Filtering.....	252
8.8.11.1	DHCP Packet Filtering.....	252
8.8.11.2	DHCP Server Packet Filtering	252
8.8.12	Debugging DHCP	253
8.9	Ethernet Ring Protection (ERP)	254
8.9.1	ERP Operation	254
8.9.2	Loss of Test Packet (LOTP).....	256
8.9.3	Configuring ERP	256
8.9.3.1	ERP Domain	256
8.9.3.2	RM Node	257
8.9.3.3	Port of ERP domain.....	257
8.9.3.4	Protected VLAN.....	257
8.9.3.5	Protected Activation.....	257
8.9.3.6	Manual Switch to Secondary.....	258
8.9.3.7	Wait-to-Restore Time.....	258
8.9.3.8	Learning Disable Time.....	258
8.9.3.9	Test Packet Interval	258
8.9.3.10	Displaying ERP Configuration	259
8.10	Stacking	260
8.10.1	Switch Group	261
8.10.2	Designating Master and Slave Switch.....	261
8.10.3	Disabling Stacking	261
8.10.4	Displaying Stacking Status	262
8.10.5	Accessing to Slave Switch from Master Switch	262
8.10.6	Sample Configuration	262
8.11	Broadcast Storm Control	265
8.12	Jumbo-frame Capacity	266
8.13	Maximum Transmission Unit (MTU).....	267
9	IP Multicast	268
9.1	Internet Group Management Protocol (IGMP)	269
9.1.1	Enabling IGMP Snooping per VLAN	269
9.1.2	IGMP v2 Snooping	270
9.1.2.1	IGMP v2 Snooping Fast Leave	271
9.1.2.2	IGMP v2 Snooping Querier	271
9.1.2.3	IGMP v2 Snooping Last-Member-Interval	272
9.1.2.4	Mrouter Port.....	273
9.1.2.5	Displaying IGMP Snooping Statistics	274
9.1.3	Multicast packets Filtering	274

9.1.4	IGMP Static Join Setting	274
9.1.5	Multicast VLAN Registration (MVR)	276
9.1.5.1	Enabling MVR.....	276
9.1.5.2	MVR Group Address.....	276
9.1.5.3	MVR IP Address	277
9.1.5.4	Send and Receive Port.....	277
9.1.5.5	Displaying MVR Configuration.....	278
9.1.6	IGMP Filtering and Profile.....	278
9.1.6.1	Creating IGMP Profile.....	278
9.1.6.2	Group Range of IGMP Profile.....	279
9.1.6.3	IGMP Profile Policy	279
9.1.6.4	Applying IGMP Profile to the Filter Port.....	279
9.1.6.5	Max Number of IGMP Join Group	280
9.2	PIM-SM (Protocol Independent Multicast-Sparse Mode)	280
9.2.1	Enables PIM Configuration.....	282
9.2.2	BSR and RP	282
9.2.2.1	Configuring Static RP.....	282
9.2.3	Bootstrap Router (BSR) Information.....	283
9.2.3.1	IP Address of candidate-BSR	283
9.2.3.2	Priority of candidate-BSR	283
9.2.3.3	Hash-mask of candidate-BSR	283
9.2.4	RP Information.....	284
9.2.4.1	IP address of Candidate RP	284
9.2.4.2	Multicast Group Registration	284
9.2.4.3	Priority of Candidate-RP	285
9.2.4.4	Interval of Candidate-RP	285
9.2.4.5	Candidate-RP Message of other members	285
9.2.5	Assert Message Information.....	286
9.2.5.1	Metric	286
9.2.5.2	Preference	286
9.2.5.3	Configuring Assert Message on specified interface	286
9.2.6	Cisco Router Interoperability	287
9.2.6.1	Checksum of Full PIM Register Message	287
9.2.7	Interval of Cache-check.....	288
9.2.8	Multicast Routing Table.....	288
9.2.9	PIM-SM on Ethernet Interface	289
9.2.9.1	PIM-SM and Sparse Mode	289
9.2.9.2	Blocking Multicast packets.....	289
9.2.9.3	Blocking Bootstrap message	289
9.2.10	Displaying PIM-SM Information	290
9.2.10.1	Multicast Routing Table.....	290
9.2.10.2	RP Table	290
9.2.10.3	PIM-SM of Ethernet Interface	290
9.2.10.4	Statistics and neighbor router	291
9.2.10.5	PIM Debug.....	291
10	IP Routing Protocol.....	292
10.1	Border Gateway Protocol (BGP)	292
10.1.1	Basic Configuration	292
10.1.1.1	BGP Routing.....	292
10.1.1.2	AS Route Filtering.....	293

10.1.1.3	BGP Filtering through Prefix Lists	293
10.1.2	Advanced Configuration	295
10.1.2.1	BGP Community Filtering	295
10.1.2.2	Displaying and Managing BGP	296
10.2	Open Shortest Path First (OSPF).....	297
10.2.1	Enabling OSPF	297
10.2.2	OSPF Network Type	297
10.2.3	OSPF Interface.....	298
10.2.3.1	Configuring Authentication	298
10.2.3.2	Configuring Authentication Key	299
10.3	Routing Information Protocol (RIP)	300
10.3.1	Enabling RIP.....	300
10.3.2	RIP Neighbor Router	301
10.3.3	RIP Version.....	301
10.3.4	Creating Static Route Available for RIP.....	302
10.3.5	Transmitting Routing Information	302
10.3.6	Metrics for Redistributed Routes	303
10.3.7	Administrative Distance	303
10.3.8	Creating Default Route	304
10.3.9	Routing Information Filtering	304
10.3.10	Routing Timer	305
10.3.11	Split-horizon	305
10.3.12	Managing Authentication Key.....	306
10.3.13	Monitoring and Managing RIP	306
11	Abbreviations	308

Illustrations

Fig. 2.1	Network Structure with hiD 6610 S311	22
Fig. 3.1	Software mode structure	26
Fig. 4.1	Process of 802.1x Authentication	59
Fig. 4.2	Multiple Authentication Servers	60
Fig. 5.1	hiD 6610 S311 Interface	68
Fig. 5.2	Port Mirroring	74
Fig. 6.1	Ping Test for Network Status	88
Fig. 6.2	IP Source Routing	89
Fig. 7.1	Weighted Round Robin	139
Fig. 7.2	Weighted Fair Queuing	140
Fig. 7.3	Strict Priority Queuing	141
Fig. 7.4	NetBIOS Filtering	148
Fig. 8.1	Port-based VLAN	173
Fig. 8.2	Example of QinQ Configuration	177
Fig. 8.3	QinQ Frame	178
Fig. 8.4	In Case Packets Going Outside in Layer 2 environment	181
Fig. 8.5	In Case External Packets Enter under Layer 2 environment (1)	181
Fig. 8.6	In Case External Packets Enter under Layer 2 environment (2)	182
Fig. 8.7	Link Aggregation	187
Fig. 8.8	Example of Loop	194
Fig. 8.9	Principle of Spanning Tree Protocol	194
Fig. 8.10	Root Switch	195
Fig. 8.11	Designated Switch	196
Fig. 8.12	Port Priority	197
Fig. 8.13	Port State	198
Fig. 8.14	Alternate Port and Backup port	199
Fig. 8.15	Example of Receiving Low BPDU	200
Fig. 8.16	Convergence of 802.1d Network	201
Fig. 8.17	Network Convergence of 802.1w (1)	201
Fig. 8.18	Network Convergence of 802.1w (2)	202
Fig. 8.19	Network Convergece of 802.1w (3)	202
Fig. 8.20	Compatibility with 802.1d (1)	203
Fig. 8.21	Compatibility with 802.1d (2)	203
Fig. 8.22	CST and IST of MSTP (1)	204
Fig. 8.23	CST and IST of MSTP (2)	205
Fig. 8.24	Example of PVSTP	211
Fig. 8.25	Root Guard	213
Fig. 8.26	Example of Layer 2 Network Design in RSTP Environment	219
Fig. 8.27	Example of Layer 2 Network Design in MSTP Environment	220
Fig. 8.28	VRRP Operation	221
Fig. 8.29	VRRP Track	226
Fig. 8.30	Rate Limit and Flood Guard	230
Fig. 8.31	DHCP Service Construction	232
Fig. 8.32	Example of DHCP Relay Agent	239
Fig. 8.33	DHCP Option 82 Operation	241
Fig. 8.34	DHCP Server Packet Filtering	253
Fig. 8.35	Ethernet Ring Protocol Operation in Failure State	254
Fig. 8.36	Ring Protection	255
Fig. 8.37	Link Failure Recovery	255

Fig. 8.38	Ring Recovery	256
Fig. 8.39	Example of Stacking.....	260
Fig. 9.1	IGMP Snooping Configuration Network	268
Fig. 9.2	PIM-SM Configuration Network.....	268
Fig. 9.3	IGMP Snooping and PIM-SM Configuration Network	269
Fig. 9.4	IP Multicasting	270
Fig. 9.5	RPT of PIM-SM	281
Fig. 9.6	STP of PIM-SM	281
Fig. 9.7	In Case Multicast Source not Directly Connected to Multicast Group	287

Tables

Tab. 1.1	Overview of Chapters	19
Tab. 1.2	Command Notation of Guide Book.....	20
Tab. 3.1	Main Commands of <i>Privileged EXEC View Mode</i>	27
Tab. 3.2	Main Commands of <i>Privileged EXEC Enable Mode</i>	27
Tab. 3.3	Main Commands of <i>Global Configuration Mode</i>	28
Tab. 3.4	Main Commands of <i>Bridge Configuration Mode</i>	29
Tab. 3.5	Main Commands of <i>Rule Configuration Mode</i>	29
Tab. 3.6	Main Commands of <i>DHCP Configuration Mode</i>	30
Tab. 3.7	Main Commands of <i>DHCP Option 82 Configuration Mode</i>	30
Tab. 3.8	Main Commands of <i>Interface Configuration Mode</i>	31
Tab. 3.9	Main Commands of <i>RMON Configuration Mode</i>	31
Tab. 3.10	Main Commands of <i>PIM Configuration Mode</i>	32
Tab. 3.11	Main Commands of <i>Router Configuration Mode</i>	32
Tab. 3.12	Main Commands of <i>VRRP Configuration Mode</i>	33
Tab. 3.13	Main Commands of <i>Route-map Configuration Mode</i>	33
Tab. 3.14	Command Abbreviation	36
Tab. 6.1	World Time Zone	77
Tab. 6.2	Options for Ping.....	86
Tab. 6.3	Options for Ping for Multiple IP Addresses.....	87
Tab. 6.4	Options for Tracing Packet Route	90
Tab. 7.1	ICMP Message Type	165
Tab. 7.2	Mask Calculation of Default Value.....	166
Tab. 7.3	Options for Packet Dump	170
Tab. 8.1	Advantages and Disadvantages of Tagged VLAN	176
Tab. 8.2	STP Path-cost	207
Tab. 8.3	RSTP Path-cost.....	207

1 Introduction

1.1 Audience

This manual is intended for SURPASS hiD 6610 S311 single-board Fast Ethernet switch operators and maintenance personnel for providers of Ethernet services. This manual assumes that you are familiar with the following:

- Ethernet networking technology and standards
- Internet topologies and protocols
- Usage and functions of graphical user interfaces.

1.2 Document Structure

Tab. 1.1 briefly describes the structure of this document.

Chapter	Description
1 Introduction	Introduces the overall information of the document.
2 System Overview	Introduces the hiD 6610 S311 system. It also lists the features of the system.
3 Command Line Interface (CLI)	Describes how to use the Command Line Interface (CLI).
4 System Connection and IP Address	Describes how to manage the system account and IP address.
5 Port Configuration	Describes how to configure the Ethernet ports.
6 System Environment	Describes how to configure the system environment and management functions.
7 Network Management	Describes how to configure the network management functions.
8 System Main Functions	Describes how to configure the system main functions.
9. IP Multicast	Describes how to configure the IP multicast packets.
10. IP Routing Protocol	Describes how to configure IP routing protocol.
11 Abbreviations	Lists all abbreviations and acronyms which appear in this document.

Tab. 1.1 Overview of Chapters

1.3 Document Convention

This guide uses the following conventions to convey instructions and information.

Information



This information symbol provides useful information when using commands to configure and means reader take note. Notes contain helpful suggestions or references.

Warning



This warning symbol means danger. You are in a situation that could cause bodily injury or broke the equipment. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents by making quick guide based on this guide.

1.4 Document Notation

The following table shows commands used in guide book. Please be aware of each command to use them correctly.

Notation	Description
a	Commands you should use as is.
NAME, PROFILE, VALUE, ...	Variables for which you supply values.
PORTS	For entry this variable, see Section 5.1.
[]	Commands or variables that appear within square brackets [] are optional.
< >	Range of number that you can use.
{ }	A choice of required keywords appears in braces { }. You must select one.
	Optional variables are separated by vertical bars .

Tab. 1.2 Command Notation of Guide Book

1.5 CE Declaration of Conformity

The CE declaration of the product will be fulfilled if the construction and cabling is undertaken in accordance with the manual and the documents listed there in, e.g. mounting instructions, cable lists where necessary account should be taken of project-specific documents.

Deviations from the specifications or unstipulated changes during construction, e.g. the use of cable types with lower screening values can lead to violation of the CE requirements. In such case the conformity declaration is invalidated and the responsibility passes to those who have caused the deviations.

1.6 GPL/LGPL Warranty and Liability Exclusion

The Siemens product, SURPASS hiD 6610 S311, contains both proprietary software and “Open Source Software”. The Open Source Software is licensed to you at no charge under the GNU General Public License (GPL) and the GNU Lesser General Public License (LGPL). This Open Source Software was written by third parties and enjoys copyright protection. You are entitled to use this Open Source Software under the conditions set out in the GPL and LGPL licenses indicated above. In the event of conflicts between Siemens license conditions and the GPL or LGPL license conditions, the GPL and LGPL conditions shall prevail with respect to the Open Source portions of the software.

The GPL can be found under the following URL:

<http://www.gnu.org/copyleft/gpl.html>

The LGPL can be found under the following URL:

<http://www.gnu.org/copyleft/lgpl.html>

The Open Source Software source code, including related copyright notices, can be found under the following URL:

<http://now-portal.c-lab.de/projects/>

In addition, if the source code to the Open Source Software has not been delivered with this product, you may obtain the source code (including the related copyright notices) by sending your request to the following e-mail address: opensrc@dasannetworks.com

You will, however, be required to reimburse Siemens for its costs of postage and copying. Any source code request made by you must be sent within 3 years of your purchase of the product. Please include a copy of your sales receipt when submitting your request. Also please include the exact name and number of the device and the version number of the installed software.

The use of Open Source Software contained in this product in any manner other than the simple running of the program occurs at your own risk, that is, without any warranty claims against Siemens. For more information about the warranties provided by the authors of the Open Source Software contained in this product, please consult the GPL and LGPL.

You have no warranty claims against Siemens when a defect in the product is or could have been caused by changes made by you in any part of the software or its configuration. In addition, you have no warranty claims against Siemens when the Open Source Software infringes the intellectual property rights of a third party.

Siemens provides no technical support for either the software or the Open Source Software contained therein if either has been changed.

You will find the GPL and LGPL license text on the SW CDR which is delivered with the product SURPASS hiD 6610 S311.

2 System Overview

SURPASS hiD 6610 S311 is a Fast Ethernet Switch provides 24 ports of 10/100Base-TX interface and 4 ports GE interface, and it supports to form a large scale network with level up integrated functions.

Integrated Layer 3 switching functions in the SURPASS hiD 6610 S311 provides various connectivity to PC, web server, LAN device, backbone device, and other switches. The SURPASS hiD 6610 S311 provides per VLAN routing, IP multicasting, IP packet filtering and DHCP.

24 ports of Fast Ethernet interface support 10/100Base-TX (RJ-45 type). 2 ports of 1000Base-X or 1000Base-FX with SFP module and 2 ports of 10/100/1000Base-TX can be used as uplink towards the core network.

The Fig. 2.1 shows network construction with using hiD 6610 S311.

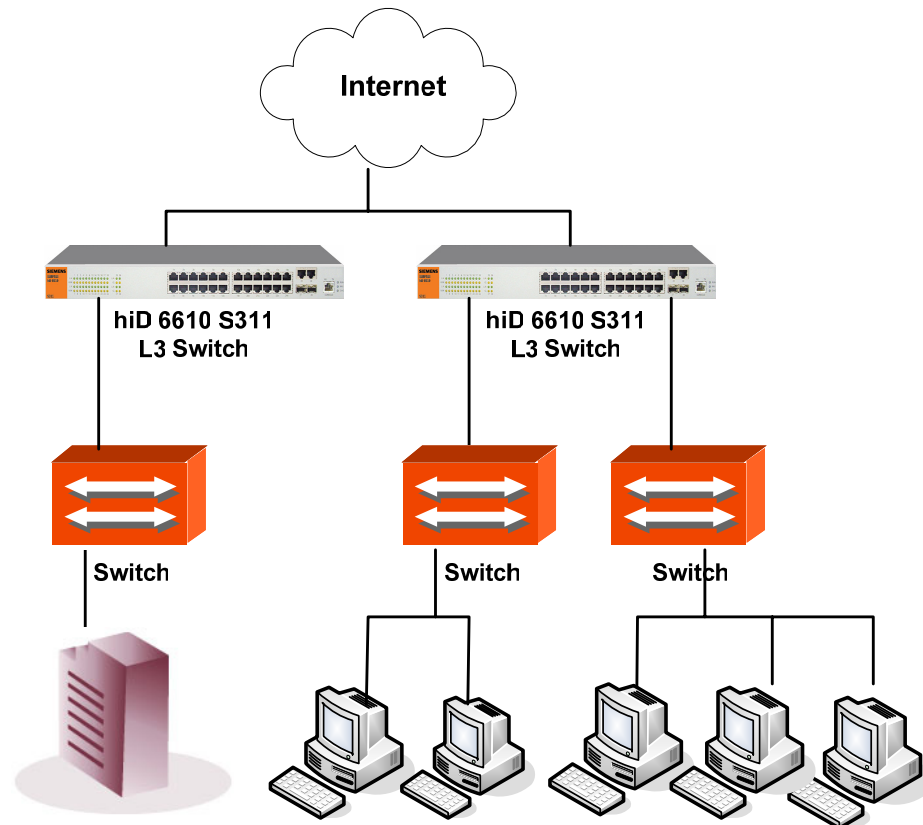


Fig. 2.1 Network Structure with hiD 6610 S311

2.1 System Features

Main features of hiD 6610 S311, having Fast Ethernet switch and Layer 3 switching function which supports both Ethernet switching and IP routing, are follow.

VLAN

Virtual Local Area Network (VLAN) is made by dividing one network into several logical networks. Packet can not be transmitted and received between different VLANs. Therefore it can prevent unnecessary packets accumulating and strengthen security. The hiD 6610 S311 recognizes 802.1q tagged frame and supports maximum 4096 VLANs and Port based, Protocol based, MAC based VLANs.

Quality of Service (QoS)

For the hiD 6610 S311, QoS-based forwarding sorts traffic into a number of classes and marks the packets accordingly. Thus, different quality of service is providing to each class, which the packets belong to. The QoS capabilities enable network managers to protect mission-critical applications and support differentiated level of bandwidth for managing traffic congestion. The hiD 6610 S311 support ingress and egress (shaping) rate limiting, and different scheduling type such as SP (Strict Priority), WRR (Weighted Round Robin) and WFQ (Weighted Fair Queuing).

Multicasting

Because broadcasting in a LAN is restricted if possible, multicasting could be used instead of broadcasting by forwarding multicast packets only to the member hosts who joined multicast group. The hiD 6610 S311 provides IGMP V2, IGMP snooping and PIM-SM for host membership management and multicast routing.

SNMP

Simple Network Management Protocol (SNMP) is to manage Network Elements using TCP/IP protocol. The hiD 6610 S311 supports SNMP version 1, 2, 3 and Remote Monitoring (RMON). Network operator can use MIB also to monitor and manage the hiD 6610 S311.

IP Routing

The hiD 6610 S311 is Layer 3 switch, which has routing table and IP address as router. Therefore, it supports static routing, RIP v1/v2, OSPF v2 and BGP v4 for unicast routing.

DHCP

The hiD 6610 S311 supports DHCP (Dynamic Host Control Protocol) Server that automatically assigns IP address to clients accessed to network. That means it has IP address pool, and operator can effectively utilize limited IP source by leasing temporary IP address. In layer 3 network, DHCP request packet can be sent to DHCP server via DHCP

relay and Option 82 function.

Spanning Tree Protocol (STP)

To prevent loop and preserve backup route in layer 2 network, the hiD 6610 S311 supports STP (802.1D). Between STP enabled switches, a root bridge is automatically selected and the network remains in tree topology. But the recovery time in STP is very slow (about 30 seconds), RSTP (Rapid Spanning Tree Protocol) is also provided. IEEE 802.1W defines the recovery time as 2 seconds. If there is only one VLAN in the network, traditional STP works. However, in more than one VLAN network, STP cannot work per VLAN. To avoid this problem, the hiD 6610 S311 supports Multiple Spanning Tree Protocol (MSTP).

Link Aggregation (Trunking)

The hiD 6610 S311 aggregates several physical interfaces into one logical port (aggregate port). Port trunk aggregates interfaces with the standard of same speed, same duplex mode, and same VLAN ID. According to IEEE 802.3ad, the hiD 6610 S311 can configure maximum 8 aggregate ports and up to 12 trunk groups.

LACP

The hiD 6610 S311 supports Link Aggregation Control Protocol (LACP), complying with IEEE 802.3ad, which aggregates multiple links of equipments to use more enlarged bandwidth.

System Management based on CLI

It is easy for users who administer system by using telnet or console port to configure the functions for system operating through CLI. CLI is easy to configure the needed functions after looking for available commands by help menu different with UNIX.

Broadcast Storm Control

Broadcast storm control is, when too much of broadcast packets are being transmitted to network, a situation of network timeout because the packets occupy most of transmit capacity. The hiD 6610 S311 supports broadcast and multicast storm control, which disuses flooding packet, that exceed the limit during the time configured by user.

RADIUS and TACACS+

hiD 6610 S311 supports client authentication protocol, that is RADIUS(Remote Authentication Dial-In User Service) and TACACS+(Terminal Access Controller Access Control System Plus). Not only user IP and password registered in switch but also authentication through RADIUS server and TACACS+ server are required to access. Therefore, security of system and network management is strengthened.

3 Command Line Interface (CLI)

This chapter describes how to use the Command Line Interface (CLI) which is used to configure the hiD 6610 S311 system.

- Command Mode
- Useful Tips

3.1 Command Mode

You can configure and manage the hiD 6610 S311 by console terminal that is installed on user's PC. For this, use the CLI-based interface commands. Connect RJ45-to-DB9 console cable to the hiD 6610 S311.

This chapter explains how CLI command mode is organized before installing. CLI command mode is consisted as follow:

- Privileged EXEC View Mode
- Privileged EXEC Enable Mode
- Global Configuration Mode
- Bridge Configuration Mode
- DHCP Configuration Mode
- DHCP Option 82 Configuration Mode
- Interface Configuration Mode
- Rule Configuration Mode
- RMON Configuration Mode
- PIM Configuration Mode
- Router Configuration Mode
- VRRP Configuration Mode
- Route-Map Configuration Mode

Fig. 3.1 shows hiD 6610 S311 software mode structure briefly.

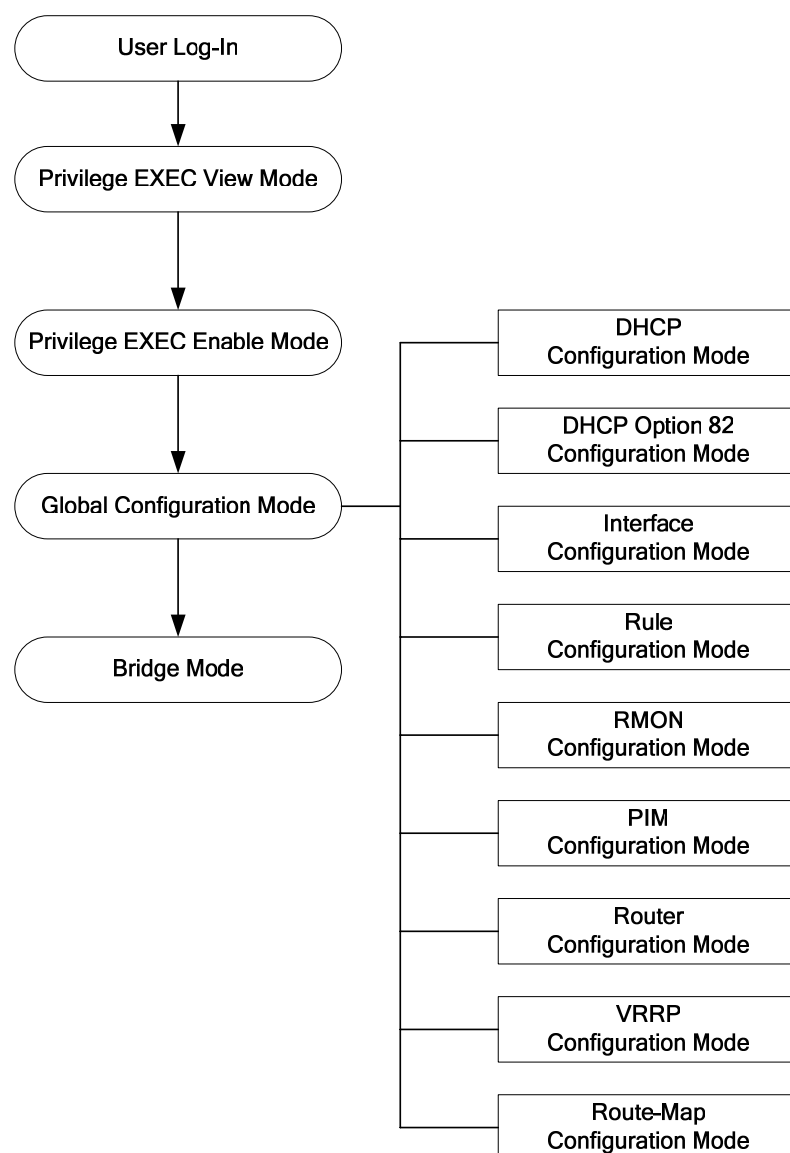


Fig. 3.1 Software mode structure

3.1.1 Privileged EXEC View Mode

When you log in to the switch, the CLI will start with *Privileged EXEC View* mode that is a read-only mode. In this mode, you can see a system configuration and information with several commands.

Tab. 3.1 shows main command of *Privileged EXEC View* mode.

Command	Description
enable	Opens <i>Privileged EXEC Enable</i> mode.
exit	Logs out the switch.
show	Shows a system configuration and information.

Tab. 3.1 Main Commands of *Privileged EXEC View* Mode

3.1.2 Privileged EXEC Enable Mode

To configure the switch, you need to open *Privileged EXEC Enable* mode with the **enable** command, then the system prompt will changes from SWITCH> to SWITCH#.

Command	Mode	Description
enable	View	Opens <i>Privileged EXEC Enable</i> mode.

You can set a password to *Privileged EXEC Enable* mode to enhance security. Once setting a password, you should enter a configured password, when you open *Privileged EXEC Enable* mode.

Tab. 3.2 shows main commands of *Privileged EXEC Enable* mode.

Command	Description
clock	Inputs time and date in system.
configure terminal	Opens Configuration mode.
telnet	Connects to another device through telnet.
terminal length	Configures the number of lines to be displayed in screen.
traceroute	Traces transmission path of packet.
where	Finds users accessed to system through telnet.

Tab. 3.2 Main Commands of *Privileged EXEC Enable* Mode

3.1.3 Global Configuration Mode

In *Global Configuration* mode, you can configure general functions of the system. You can also open another configuration mode from this mode.

To open *Global Configuration* mode, enter the **configure terminal** command, and then the system prompt will be changed from SWITCH# to SWITCH(config)#.

Command	Mode	Description
configure terminal	Enable	Opens <i>Global Configuration</i> mode from <i>Privileged EXEC Enable</i> mode.

Tab. 3.3 shows a couple of important main commands of Global Configuration mode.

Command	Description
access-list	Configures policy to limit routing information on the standard of AS.
arp	Registers IP address and MAC address in ARP table.
bgp	Helps BGP configuration.
bridge	Opens <i>Bridge Configuration</i> mode.
copy	Makes a backup file for the configuration of the switch.
dot1x	Configures various functions of 802.1x daemon.
end	Closes current mode and returns to <i>User EXEC</i> mode.
exit	Closes current mode and returns to previous mode.
hostname	Changes host name of the switch.
exec-timeout	Configures auto-logout function.
fan	Configures fan operation
interface	Opens <i>Interface Configuration</i> mode.
ip	Configures various functions of the interface.
passwd	Changes a system password.
qos	Configures QoS.
restore factory-defaults	Restores the default configuration of the switch.
rmon-alarm	Opens <i>Rmon-alarm</i> configuration mode.
rmon-event	Opens <i>Rmon-event</i> configuration mode.
rmon-history	Opens <i>Rmon-history</i> configuration mode.
route-map	Opens <i>Route-map Configuration</i> mode.
router	Opens <i>Router Configuration</i> mode.(OSPF, RIP, VRRP, PIM, BGP)
snmp	Configures SNMP.
sntp	Configures SNTP
syslog	Configures syslog.
time-zone	Configures time zone.

Tab. 3.3 Main Commands of *Global Configuration* Mode

3.1.4 Bridge Configuration Mode

In *Bridge Configuration* mode, you can configure various Layer 2 functions such as VLAN, STP, LACP, EFM OAM, etc.

To open *Bridge Configuration* mode, enter the **bridge** command, then the system prompt will be changed from SWITCH(config)# to SWITCH(bridge)#.

Command	Mode	Description
bridge	Global	Opens <i>Bridge Configuration</i> mode.

Tab. 3.4 shows a couple of main commands of *Bridge Configuration* mode.

Command	Description
auto-reset	Configures the system for automatic rebooting
dhcp-server-filter	Configures packet filtering of DHCP server.
erp	Configures ERP function
lACP	Configures LACP function.
lldp	Configures LLDP function
mac	Manages MAC address
mac-flood-guard	Configures mac-flood-guard.
mirror	Configures mirroring function.
oam	Configures EFM-OAM protocol
port	Sets port configuration
stp	Configures Spanning Tree Protocol
trunk	Configures trunk-function.
vlan	Configures VLAN function.

Tab. 3.4 Main Commands of *Bridge Configuration* Mode

3.1.5 Rule Configuration Mode

You can open *Rule Configuration* mode using the command, **rule NAME create**, on *Global Configuration* mode.

If you open *Rule Configuration* mode, the system prompt is changed from SWITCH(config)# to SWITCH(config-rule[name])#.

Command	Mode	Description
rule NAME create	Global	Opens <i>Rule Configuration</i> mode.

On the *Rule Configuration* mode, it is possible to configure the condition and operational method for the packets to which the rule function is applied.

Tab. 3.5 shows a couple of important main commands of *Rule Configuration* mode.

Command	Description
apply	Configures rule configuration and applies it to the switch.
mac	Configures a packet condition by MAC address.
match	Configures an operational condition which meets the packet condition.
port	Configures a packet condition by port number.
priority	Configures the priority for rule.
vlan	Configures VLAN.

Tab. 3.5 Main Commands of *Rule Configuration* Mode

3.1.6 DHCP Configuration Mode

To open *DHCP Configuration* mode, use the command, **ip dhcp pool POOL**, on *Global Configuration* mode as follow. Then the prompt is changed from SWITCH(config)# to SWITCH(config-dhcp[POOL])#.

Command	Mode	Description
ip dhcp pool POOL	Global	Opens <i>DHCP Configuration</i> mode to configure DHCP.

DHCP Configuration mode is to configure range of IP address used in DHCP server, group in subnet, and default gateway of subnet.

Command	Description
default-gateway	Configures a default gateway of subnet.
dns-server	Configures DNS server.
range	Configures a range of IP address used in DHCP server.
subnet	Configures a subnet

Tab. 3.6 Main Commands of *DHCP Configuration* Mode

3.1.7 DHCP Option 82 Configuration Mode

To open *DHCP Option 82 Configuration* mode, use the command, **ip dhcp option82**, on *Global Configuration* mode as follow. Then the prompt is changed from SWITCH(config)# to SWITCH(config-opt82)#.

Command	Mode	Description
ip dhcp option82	Global	Opens <i>DHCP Option 82 Configuration</i> mode for DHCP option 82 configuration.

On *DHCP Option 82 Configuration* mode, configure a range of IP address used in DHCP server and designate the group in subnet and configure default gateway of the subnet. Tab. 3.7 is the main commands of *DHCP Option 82 Configuration* mode of hiD 6610 S311.

Command	Description
policy	Configures a rule for option 82 packet.
remote-id	Configures a remote ID.
system-remote-id	Configures the remote ID of the system.
system-circuit-id	Configures the circuit ID of the system.

Tab. 3.7 Main Commands of *DHCP Option 82 Configuration* Mode

3.1.8 Interface Configuration Mode

To open *Interface Configuration* mode, enter the command, **interface** *INTERFACE*, on *Global Configuration* mode, and then the prompt is changed from SWITCH(config)# to SWITCH(config-if)#.

Command	Mode	Description
interface <i>INTERFACE</i>	Global	Opens <i>Interface Configuration</i> mode.

Interface Configuration mode is to assign IP address in Ethernet interface and to activate or deactivate interface.

Tab. 3.8 shows a couple of main commands of *Interface Configuration* mode.

Command	Description
bandwidth	Configures bandwidth used to make routing information.
description	Makes description of interface.
ip	Assigns IP address.
shutdown	Deactivates interface.
mtu	Sets MTU value to interface.

Tab. 3.8 Main Commands of *Interface Configuration* Mode

3.1.9 RMON Configuration Mode

To open *RMON-Alarm Configuration* mode, enter **rmon-alarm** <1-65534>. To open *RMON-Event Configuration* mode, input **rmon-event** <1-65534>. And to open *RMON-History Configuration* mode, enter **rmon-history** <1-65534>.

Tab. 3.9 shows a couple of important main commands of *RMON Configuration* mode.

Command	Description
active	Enables each RMON configuration.
community	Configures password for trap message transmission right.
description	Describes the RMON event.
falling-event	Configures to generate RMON alarm when object is less than configured threshold.
falling-threshold	Defines the falling threshold
owner	Shows the subject, which configures each RMON and uses related information.
rising-event	Configures to generate RMON alarm when object is more than configured threshold.
requested-buckets	Defines a bucket count for the interval.

Tab. 3.9 Main Commands of *RMON Configuration* Mode

3.1.10 PIM Configuration Mode

To open *PIM Configuration* mode, enter the following command. The system prompt is changed from SWITCH(config)# to SWITCH(config-router)#.

Command	Mode	Description
router pim	Global	Opens <i>PIM Configuration</i> mode.

Tab. 3.10 shows a couple of important main commands of *PIM Configuration* mode.

Command	Description
cache-check	Configures the interval that checks packet transmission result from source.
cand-bsr	Configures information for candidate-BSR.
cand-rp	Configures information for candidate-RP.
metric	Configures metric to decide Assert.
mroute	Configures multicast routing table
preference	Configures preference to decide Assert.
static-rp	Configures RP by user manually.
whole-packet-checksum	Gives compatibility with Cisco router when transmitting Register message.

Tab. 3.10 Main Commands of *PIM Configuration* Mode

3.1.11 Router Configuration Mode

To open *Router Configuration* mode, use the following command. The system prompt is changed from SWITCH(config)# to SWITCH(config-router)#.

Command	Mode	Description
router IP-PROTOCOL	Global	Opens <i>Router Configuration</i> mode.

According to routing protocol way, *Router Configuration* mode is divided into BGP, RIP, and OSPF. They are used to configure each IP routing protocol.

Tab. 3.11 shows a couple of main commands of *Router Configuration* mode.

Command	Description
distance	Configures distance value to find better route.
neighbor	Configures neighbor router.
network	Configures network to operate each routing protocol.
redistribute	Registers transmitted routing information to another router's table.

Tab. 3.11 Main Commands of *Router Configuration* Mode

3.1.12 VRRP Configuration Mode

To open *VRRP Configuration* mode, use the following command. The system prompt is changed from SWITCH(config)# to SWITCH(config-router)#.

Command	Mode	Description
router vrrp <i>INTERFACE GROUP-ID</i>	Global	Opens <i>VRRP Configuration</i> mode.

Tab. 3.12 shows a couple of main commands of *Router Configuration* mode.

Command	Description
associate	Configures associated IP address same with virtual router.
authentication	Configures password of virtual router group.
preempt	Activates/deactivates preempt.
track	Configures VRRP track.
vip-access	Configures the function of accessing associated IP address.
vr-priority	Assigns priority to virtual router.
vr-timers	Configures advertisement time, which means the interval that master router distributes its information to another virtual router.

Tab. 3.12 Main Commands of *VRRP Configuration* Mode

3.1.13 Route-Map Configuration Mode

To open *Route-map Configuration* mode, use the following command. The prompt is changed from SWITCH(config)# to SWITCH(config-route-map)#.

Command	Mode	Description
route-map <i>NAME</i> { permit deny } <1-65535>	Global	Opens <i>Route-map Configuration</i> mode.

On *Route-map Configuration* mode, you can configure the place where information is from and sent in routing table.

Tab. 3.13 shows a couple of important main commands of *Route-map Configuration* mode.

Command	Description
match	Transmits routing information to specified place.
set	Configures router address and distance.

Tab. 3.13 Main Commands of *Route-map Configuration* Mode

3.2 Useful Tips

This section provides useful functions for user's convenience while using CLI commands. They are as follow.

- Listing Available Commands
- Calling Command History
- Using Abbreviation
- Using Command of Privileged EXEC Enable Mode
- Exit Current Command Mode

3.2.1 Listing Available Commands

To list available commands, input question mark <?>. When you input the question mark <?> in each command mode, you can see available commands used in this mode and variables following after the commands.

The following is the available commands on *Privileged EXEC Enable* mode of the hiD 6610 S311.

```
SWITCH# ?
Exec commands:
clear          Reset functions
clock          Manually set the system clock
configure      Enter configuration mode
copy           Copy from one file to another
debug          Debugging functions (see also 'undebug')
enable         Turn on privileged mode command
exit           End current mode and down to previous mode
help           Description of the interactive help system
no             Negate a command or set its defaults
ping           Send echo messages
show           Show running system information
telnet         Open a telnet connection
terminal       Set terminal line parameters
traceroute     Trace route to destination
where          List active user connections
write          Write running configuration to memory, network, or terminal
SWITCH#
```



Question mark <?> will not be seen in the screen and you do not need to press <ENTER> key to display commands list.

If you need to find out the list of available commands of the current mode in detail, use the following command.

Command	Mode	Description
show list	All	Shows available commands of the current mode.
show cli		Shows available commands of the current mode with tree structure.

The following is an example of displaying list of available commands of *Privileged EXEC Enable* mode.

```
SWITCH# show list

clear arp IFNAME
clear arp-inspection mapping counter
clear arp-inspection statistics
clear cpu statistics (PORTS|)
clear ip bgp *
clear ip bgp * in
clear ip bgp * in prefix-filter
clear ip bgp * ipv4 (unicast|multicast) in
clear ip bgp * ipv4 (unicast|multicast) in prefix-filter
clear ip bgp * ipv4 (unicast|multicast) out
clear ip bgp * ipv4 (unicast|multicast) soft
clear ip bgp * ipv4 (unicast|multicast) soft in
clear ip bgp * ipv4 (unicast|multicast) soft out
clear ip bgp * out
clear ip bgp * soft
clear ip bgp * soft in
clear ip bgp * soft out
clear ip bgp * vpnv4 unicast in
clear ip bgp * vpnv4 unicast out
clear ip bgp * vpnv4 unicast soft
clear ip bgp * vpnv4 unicast soft in
clear ip bgp * vpnv4 unicast soft out
-- more --
```



Press the <ENTER> key to skip to the next list.

In case of the hiD 6610 S311 installed command shell, you can find out commands starting with specific alphabet. Input the first letter and question mark without space. The following is an example of finding out the commands starting “s” in *Privileged EXEC Enable* mode of hiD 6610 S311.

```
SWITCH# s?
show          Show running system information
SWITCH# s
```

Also, it is possible to view variables you should input following after commands. After inputting the command you need, make one space and input question mark. The following is an example of viewing variables after the command, **write**. Please note that you must make one space after inputting.

```
SWITCH# write ?
file          Write to file
memory        Write to NV memory
terminal      Write to terminal
<cr>

SWITCH# write
```

3.2.2 Calling Command History

In case of installed command shell, you do not have to enter repeated command again. When you need to call command history, use this arrow key <↑>. When you press the arrow key, the latest command you used will be displayed one by one.

The following is an example of calling command history after using several commands. After using these commands in order: **show clock** → **configure terminal** → **interface 1** → **exit**, press the arrow key <↑> and then you will see the commands from latest one: **exit** → **interface 1** → **configure terminal** → **show clock**.

```
SWITCH(config)# exit
SWITCH# show clock
Mon, 5 Jan 1970 23:50:12 GMT+0000
SWITCH# configure terminal
SWITCH(config)# interface 1
SWITCH(config-if)# exit
SWITCH(config)# exit
SWITCH# (press the arrow key ↑)
↓
SWITCH# exit (arrow key ↑)
↓
SWITCH# interface 1 (arrow key ↑)
↓
SWITCH# configure terminal (arrow key ↑)
↓
SWITCH# show clock (arrow key ↑)
```

The hiD 6610 S311 also provides the command that shows the commands used before up to 100 lines.

Command	Mode	Description
show history	Enable	Shows a command history.

3.2.3 Using Abbreviation

Most of the commands can be used also with abbreviated form. The following table shows some examples of abbreviated commands.

Command	Abbreviation
clock	cl
exit	ex
show	sh
configure terminal	con te

Tab. 3.14 Command Abbreviation

3.2.4 Using Command of Privileged EXEC Enable Mode

You can execute the commands of *Privileged EXEC Enable* mode as **show**, **ping**, **telnet**, **traceroute**, and so on regardless of which mode you are located on.

To execute the commands of *Privileged EXEC Enable* mode on another mode, use the following command.

Command	Mode	Description
do <i>COMMAND</i>	All	Executes the commands of <i>Privileged EXEC</i> mode.

3.2.5 Exit Current Command Mode

To exit to the previous command mode, use the following command.

Command	Mode	Description
exit	All	Exits to the previous command mode.
end		Exits to <i>Privileged EXEC enable</i> mode.



If you use the command, **exit**, on *Privileged EXEC View* mode or *Privileged EXEC Enable* mode, you will be logged out!

4 System Connection and IP Address

4.1 System Connection

After installing switch, the hiD 6610 S311 is supposed to examine that each port is rightly connected to network and management PC. And then, user connects to system to configure and manage the hiD 6610 S311. This section provides instructions how to change password for system connection, connect to system through telnet as the following order.

- System Login
- Password for Privileged EXEC Mode
- Changing Login Password
- Management for System Account
- Limiting Number of User
- Telnet Access
- Auto Log-out
- System Rebooting

4.1.1 System Login

After installing the hiD 6610 S311, finally make sure that each port is correctly connected to PC for network and management. And then, turn on the power and boot the system as follow.

Step 1

When you turn on the switch, booting will be automatically started and login prompt will be displayed.

```
SWITCH login:
```

Step 2

When you enter login ID at the login prompt, password prompt will be displayed. And enter password to open *Privileged EXEC View* mode. By default setting, login ID is configured as *admin* and it is possible to access without password.

```
SWITCH login: admin
Password:
SWITCH>
```

Step 3

In *Privileged EXEC View* mode, you can check only the configuration for the switch. To configure and manage the switch, you should begin *Privileged EXEC Enable* mode. The following is an example of beginning *Privileged EXEC Enable* mode.

```
SWITCH> enable
SWITCH#
```

4.1.2 Password for Privileged EXEC Mode

You can configure a password to enhance the security for *Privileged EXEC Enable* mode. To configure a password for *Privileged EXEC Enable* mode, use the following command.

Command	Mode	Description
passwd enable <i>PASSWORD</i>	Global	Configures a password to begin <i>Privileged EXEC Enable</i> mode.
passwd enable 8 <i>PASSWORD</i>		Configures an encrypted password.



password enable does not support encryption at default value. Therefore, it shows the string (or password) as it is when you use the **show running-config** command. In this case, the user's password shown to everyone and has insecure environment.

To encrypt the password which will be shown at running-config, you should use the **service password-encryption** command. And to represent the string (password) is encrypted, input **8** before the encrypted string.

When you use the **password enable** command with **8** and "the string", you will make into *Privileged EXEC Enable* mode with the encrypted string. Therefore, to log in the system, you should do it with the encrypted string as password that you configured after **8**. In short, according to using the **8** option or not, the next string is encrypted or not.

The following is an example of configure the password in *Privileged EXEC Enable* mode as *testpassword*.

```
SWITCH# configure terminal
SWITCH(config)# passwd enable testpassword
SWITCH(config)#
```

The following is an example of accessing after configuring the password.

```
SWITCH login: admin
Password:
SWITCH > enable
Password:
SWITCH#
```

To delete the configured password, use the following command.

Command	Mode	Description
no passwd enable	Global	Deletes the password.

The created password can be displayed with the command, **show running-config**. To encrypt the password not to be displayed, use the following command.

Command	Mode	Description
service password-encryption	Global	Encrypts system password.

To disable password encryption, use the following command.

Command	Mode	Description
no service password-encryption	Global	Disables password encryption.

4.1.3 Changing Login Password

To configure a password for created account, use the following command.

Command	Mode	Description
passwd [NAME]	Global	Configures a password for created account.

The following is an example of changing password.

```
SWITCH(config)# passwd Siemens
Changing password for Siemens
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password: junior95
Re-enter new password: junior95
Password changed.
SWITCH(config)#
```



The password you are entering won't be seen in the screen, so please be careful not to make mistake.

4.1.4 Management for System Account

4.1.4.1 Creating System Account

For the hiD 6610 S311, the administrator can create a system account. In addition, it is possible to set the security level from 0 to 15 to enhance the system security.

To create a system account, use the following command.

Command	Mode	Description
user add NAME DESCRIPTION	Global	Creates a system account.
user add NAME level <0-15> DESCRIPTION		Creates a system account with a security level.



The account of level 0 to level 14 without any configuring authority only can use **exit** and **help** in *Privileged EXEC View* mode and cannot access to *Privileged EXEC Enable* mode. The account with the highest level 15 has a read-write authority.

To delete the created account, use the following command.

Command	Mode	Description
user del <i>NAME</i>	Global	Delete the created account.

To display the created account, use the following command.

Command	Mode	Description
show user	Enable/Global	Shows the created account.

4.1.4.2 Configuring Security Level

For the hiD 6610 S311, it is possible to configure the security level from 0 to 15 for a system account. The level 15, as the highest level, has a read-write authority. The administrator can configure from level 0 to level 14. The administrator decides which level user uses which commands in which level. As the basic right from level 0 to level 14, it is possible to use **exit** and **help** command in *Privileged EXEC Enable* mode and it is not possible to access to *Privileged EXEC Enable* mode.

To define the security level and its authority, use the following command.

Command	Mode	Description
privilege bgp level <0-15> { <i>COMMAND</i> all }	Global	Uses the specific command of <i>BGP Configuration</i> mode in the level.
privilege bridge level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>Bridge Configuration</i> mode in the level.
privilege configure level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>Global Configuration</i> mode in the level.
privilege dhcp-option82 level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>DHCP Option 82 Configuration</i> mode in the level.
privilege dhcp-pool level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>DHCP Configuration</i> mode in the level.
privilege enable level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>Privileged EXEC</i> mode in the level.
privilege interface level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>Interface Configuration</i> mode in the level.
privilege ospf level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>OSPF Configuration</i> mode in the level.
privilege pim level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>PIM Configuration</i> mode in the level.
privilege rip level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>RIP Configuration</i> mode in the level.
privilege rmon-alarm level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>RMON Configuration</i> mode in the level.
privilege rmon-event level <0-15> { <i>COMMAND</i> all }		

Command	Mode	Description
privilege rmon-history level <0-15> { <i>COMMAND</i> all }	Global	Uses the specific command of <i>RMON Configuration</i> mode in the level.
privilege route-map level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>Route-map Configuration</i> mode in the level.
privilege rule level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>Rule Configuration</i> mode in the level.
privilege view level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>User EXEC</i> mode in the level.
privilege vrrp level <0-15> { <i>COMMAND</i> all }		Uses the specific command of <i>VRRP Configuration</i> mode in the level.

The commands that are used in low level can be also used in the higher level. For example, the command in level 0 can be used in from level 0 to level 14.

The commands should be input same as the displayed commands by **show list**. Therefore, it is not possible to input the commands in the bracket separately.

```
SWITCH# show list
clear arp-inspection mapping counter
clear arp-inspection statistics
clear cpu statistics (PORTS|)
clear ip bgp *
clear ip bgp * in
clear ip bgp * in prefix-filter
clear ip bgp * ipv4 (unicast|multicast) in
clear ip bgp * ipv4 (unicast|multicast) in prefix-filter
clear ip bgp * ipv4 (unicast|multicast) out
clear ip bgp * ipv4 (unicast|multicast) soft
clear ip bgp * ipv4 (unicast|multicast) soft in
clear ip bgp * ipv4 (unicast|multicast) soft out
clear ip bgp * out
clear ip bgp * soft
clear ip bgp * soft in
clear ip bgp * soft out
clear ip bgp * vpnv4 unicast in
clear ip bgp * vpnv4 unicast out
clear ip bgp * vpnv4 unicast soft
clear ip bgp * vpnv4 unicast soft in
clear ip bgp <1-65535> out
clear ip bgp <1-65535> soft
clear ip bgp <1-65535> soft in
clear ip bgp <1-65535> soft out
clear ip bgp <1-65535> vpnv4 unicast in
clear ip bgp <1-65535> vpnv4 unicast out
clear ip bgp <1-65535> vpnv4 unicast soft
--More--
(Omitted)
```

It is not possible to input **clear ip bgp * ipv4 unicast in**. You should input like **clear ip bgp * ipv4 {unicast | multicast} in**.

The commands starting with the same character are applied by inputting only the starting commands. For example, if you input **show**, all the commands starting with **show** are applied.

To delete a configured security level, use the following command.

Command	Mode	Description
no privilege	Global	Deletes all configured security levels.
no privilege bgp level <0-15> { <i>COMMAND</i> all }		Delete a configured security level on each mode.
no privilege bridge level <0-15> { <i>COMMAND</i> all }		
no privilege configure level <0-15> { <i>COMMAND</i> all }		
no privilege dhcp-option82 level <0-15> { <i>COMMAND</i> all }		
no privilege dhcp-pool level <0-15> { <i>COMMAND</i> all }		
no privilege enable level <0-15> { <i>COMMAND</i> all }		
no privilege interface level <0-15> { <i>COMMAND</i> all }		
no privilege ospf level <0-15> { <i>COMMAND</i> all }		
no privilege pim level <0-15> { <i>COMMAND</i> all }		
no privilege rip level <0-15> { <i>COMMAND</i> all }		
no privilege rmon-alarm level <0-15> { <i>COMMAND</i> all }		
no privilege rmon-event level <0-15> { <i>COMMAND</i> all }		
no privilege rmon-history level <0-15> { <i>COMMAND</i> all }		
no privilege route-map level <0-15> { <i>COMMAND</i> all }		
no privilege rule level <0-15> { <i>COMMAND</i> all }		
no privilege view level <0-15> { <i>COMMAND</i> all }		
no privilege vrrp level <0-15> { <i>COMMAND</i> all }		

To display a configured security level, use the following command.

Command	Mode	Description
show privilege	View	Shows a configured security level.
show privilege now	Enable Global	Shows a security level of current mode.

The following is an example of creating the system account *test0* having a security level 10 and *test1* having a security level 1 without password.

```
SWITCH(config)# user add test0 level 0 level0user
Changing password for test0
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:(Enter)
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password: (Enter)
Password changed.
SWITCH(config)# user add test1 level 1 levelluser
Changing password for test1
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password: (Enter)
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password: (Enter)
Password changed.
SWITCH(config)# show user
=====
User name           Description           Level
=====
test0                level0user           0
test1                levelluser           1
SWITCH(config)#
```

The following is an example of configuring an authority of the security level 0 and 1.

```
SWITCH(config)# privilege view level 0 enable
SWITCH(config)# privilege enable level 0 show
SWITCH(config)# privilege enable level 1 configure terminal
SWITCH(config)# show privilege

Command Privilege Level Configuration
-----
Node      All  Level  Command
EXEC(ENABLE)      1  configure terminal
EXEC(VIEW)        0  enable
EXEC(ENABLE)      0  show
3 entry(s) found.
SWITCH(config)#
```


In the above configuration, as level 0, it is possible to use only show command in *Privileged EXEC Enable* mode; however as level 1, it is possible to use not only the commands in level 1 but also time configuration commands in *Privileged EXEC Enable* mode and accessing commands to *Global Configuration* mode.

4.1.5 Limiting Number of User

For hiD 6610 S311, you can limit the number of user accessing the switch through both console port and telnet. In case of using the system authentication with RADIUS or TACACS+, the configured number includes the number of user accessing the switch via the authentication server.

To set the number of user accessing the switch, use the following command.

Command	Mode	Description
login connect <1-8>	Global	Sets the number of user accessing the switch. Default: 8

4.1.6 Telnet Access

To connect to the host through telnet at remote place, use the following command.

Command	Mode	Description
telnet DESTINATION [TCP-PORT]	Enable	Connects to a remote host. DESTINATION: IP address or host name



In case of telnet connection, you should wait for **[OK]** message, when you save a system configuration. Otherwise, all changes will be deleted when the telnet session is disconnected.

```
SWITCH# write memory
[OK]
SWITCH#
```

The system administrator can disconnect users connected from remote place. To disconnect a user connected through telnet, use the following command.

Command	Mode	Description
disconnect TTY-NUMBER	Enable	Disconnects a user connected through telnet.

The following is an example of disconnecting a user connected from a remote place.

```
SWITCH# where
admin at from console for 4 days 22 hours 15 minutes 24.88 seconds
admin at tty0 from 10.0.1.4:1670 for 4 days 17 hours 53 minutes 28.76 seconds
admin at tty1 from 147.54.140.133:49538 for 6 minutes 34.12 seconds
SWITCH# disconnect tty0
SWITCH# where
admin at from console for 4 days 22 hours 15 minutes 34.88 seconds
admin at tty1 from 147.54.140.133:49538 for 6 minutes 44.12 seconds
SWITCH#
```

4.1.7 Auto Log-out

For security reasons of the hiD 6610 S311, if no command is entered within the configured inactivity time, the user is automatically logged out of the system. Administrator can configure the inactivity timer.

To enable auto-logout function, use the following command.

Command	Mode	Description
exec-timeout <1-35791> [<0-59>]	Global	Enables auto log-out. 1-35791: time unit in minutes (by default 10 minutes) 0-59: time unit in seconds
exec-timeout 0		Disables auto log-out.

To display a configuration of auto-logout function, use the following command.

Command	Mode	Description
show exec-timeout	Enable Global	Shows a configuration of auto-logout function.

The following is an example of configuring auto-logout function as 60 seconds and viewing the configuration.

```
SWITCH(config)# exec-timeout 60
SWITCH(config)# show exec-timeout
Log-out time : 60 seconds
SWITCH(config)#
```

4.1.8 System Rebooting

4.1.8.1 Manual System Rebooting

When installing or maintaining the system, some tasks require rebooting the system by various reasons. Then you can reboot the system with a selected system OS.

To restart the system manually, use the following command.

Command	Mode	Description
reload [os1 os2]	Enable	Restarts the system.

If you reboot the system without saving new configuration, new configuration will be deleted. So, you have to save the configuration before rebooting. Not to make that mistake, hiD 6610 S311 is supported to print the following message to ask if user really wants to reboot and save configuration.

If you want to continue to reboot, press <y> key, if you want to save new configuration, press <n> key.

```
SWITCH# reload
```

Do you want to save the system configuration? [y/n]]

4.1.8.2 Auto System Rebooting

The hiD 6610 S311 reboots the system according to user's configuration. There are two basises for system rebooting. These are CPU and memory. CPU is rebooted in case CPU Load or Interrupt Load continues for the configured time. Memory is automatically rebooted in case memory low occurs as the configured times.

To enable auto system rebooting function, use the following command.

Command	Mode	Description
auto-reset cpu <70-100> <1-100> <i>TIME</i>	Bridge	Configure to reboot the system automatically in case an average of CPU or interrupt load exceeds the configured value during the user-defined time. 70-100: average of CPU load per 1 minute 1-100: average of interrupt load TIME: minute
auto-reset memory <1-120> <1-10>		Configure to reboot the system automatically in case memory low occurs as the configured value. 1-120: time of memory low 1-10: count of memory low(The default is 5)
no auto-reset {cpu memory}		Disables auto system rebooting.

To show auto system rebooting configuration, use the following command.

Command	Mode	Description
show auto-reset {cpu memory}	Global/ Bridge	Shows a configuration of auto-rebooting function.

The following is an example of configuring auto-restarting function in case CPU load or Interrupt load maintains over 70% during 60 seconds and viewing the configuration.

```
SWITCH(config)# SWITCH(bridge)# auto-reset cpu 70 70 1
SWITCH(bridge)# show auto-reset cpu
-----
Auto-Reset Configuration(CPU)
-----
auto-reset:          on
cpu load:            70
interrupt load:      70
continuation time:   1
SWITCH(bridge)#
```

4.2 System Authentication

For the enhanced system security, the hiD 6610 S311 provides two authentication methods to access the switch using Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+).

4.2.1 Authentication Method

To set the system authentication method, use the following command.

Command	Mode	Description
login {local remote} {radius tacacs host all} enable	Global	Set the system authentication method. local: authentication for console access remote: authentication for telnet access radius: selects RADIUS authentication. tacacs: selects TACACS+ authentication. host: selects nominal system authentication (default). all: selects all the authentication methods.
login {local remote} {radius tacacs host all} disable		Disables a configured system authentication method.

4.2.2 Authentication Interface

If more than 2 interfaces are specified to the hiD 6610 S311, you can designate one specific interface to access RADIUS or TACACS server.

To designate an authentication interface, use the following command.

Command	Mode	Description
login {radius tacacs} interface INTERFACE [A.B.C.D]	Global	Designates an authentication interface. radius: selects RADIUS authentication. tacacs: selects TACACS+ authentication. INTERFACE: interface name A.B.C.D: IP address (optional)

4.2.3 Primary Authentication Method

You can set the order of the authentication method with giving the priority to each authentication method.

To set the primary authentication method, use the following command

Command	Mode	Description
login {local remote} {radius tacacs host} primary	Global	Set the primary authentication method. local: authentication for console access remote: authentication for telnet access radius: selects RADIUS authentication. tacacs: selects TACACS+ authentication. host: selects nominal system authentication (default).

4.2.4 RADIUS Server

4.2.4.1 RADIUS Server for System Authentication

To add/delete the RADIUS server for system authentication, use the following command.

Command	Mode	Description
login radius server add <i>A.B.C.D</i> <i>KEY</i>	Global	Adds the RADIUS server with its information. A.B.C.D: RADIUS server address KEY: authentication key value
login radius server add <i>A.B.C.D</i> <i>KEY auth_port PORT acct_port</i> <i>PORT</i>		Adds the RADIUS server with its information. A.B.C.D: RADIUS server address KEY: authentication key value auth_port: Enters authentication port number(optional) acct_port: Enters accounting port number(optional)
login radius server del <i>A.B.C.D</i>		Deletes an added RADIUS server.



You can add up to 5 RADIUS servers.

4.2.4.2 RADIUS Server Priority

To specify the priority of a registered RADIUS server, use the following command.

Command	Mode	Description
login radius server move <i>A.B.C.D <1-5></i>	Global	Specifies the priority of RADIUS server. A.B.C.D: IP address 1-5: priority of RADIUS server

4.2.4.3 Timeout of Authentication Request

After the authentication request, the hiD 6610 S311 waits for the response from the RADIUS server for specified time.

To specify a timeout value, use the following command.

Command	Mode	Description
login radius timeout <i><1-100></i>	Global	Specifies a timeout value. 1-100: waiting-time for the response (default: 3)

4.2.4.4 Frequency of Retransmit

If there is no response from RADIUS server, the hiD 6610 S311 is supposed to retransmit an authentication request. To set the frequency of retransmitting an authentication request, use the following command.

Command	Mode	Description
login radius retransmit <i><1-10></i>	Global	Sets the frequency of retransmit. 1-10: Enters the times of retry (default: 3)

4.2.5 TACACS Server

4.2.5.1 TACACS Server for System Authentication

To add/delete the TACACS server for system authentication, use the following command.

Command	Mode	Description
login tacacs server add <i>A.B.C.D</i> <i>KEY</i>	Global	Adds the TACACS server with its information. A.B.C.D: IP address KEY: authentication key value
login tacacs server del <i>A.B.C.D</i>		Deletes an added TACACS server. A.B.C.D: IP address



You can add up to 5 TACACS servers.

4.2.5.2 TACACS Server Priority

To specify the priority of a registered TACACS server, use the following command.

Command	Mode	Description
login tacacs server move <i>A.B.C.D</i> <1-5>	Global	Specifies the priority of RADIUS server. A.B.C.D: TACACS server address 1-5: the priority of TACACS server

4.2.5.3 Timeout of Authentication Request

After the authentication request, the hiD 6610 S311 waits for the response from the TACACS server for specified time.

To specify a timeout value, use the following command.

Command	Mode	Description
login tacacs timeout <1-100>	Global	Specifies a timeout value. 1-100: waiting-time for the response (default: 5)

4.2.5.4 Additional TACACS+ Configuration

The hiD 6610 S311 provides several additional options to configure the system authentication via TACACS server.

TCP Port for the Authentication

To specify TCP port for the system authentication, use the following command.

Command	Mode	Description
login tacacs socket-port <1-65535>	Global	Specifies TCP port for the authentication. 1-65535: TCP port

Authentication Type

To select the authentication type for TACACS+, use the following command.

Command	Mode	Description
login tacacs auth-type {ascii pap chap}	Global	Selects the authentication type for TACACS+. ascii: plain text pap: password authentication protocol chap: challenge handshake authentication protocol

Priority Level

You can define a priority level of user. According to the defined priority level, the user has different authorization to access the DSLAM. This priority should be defined in the TACACS server in the same way.

To define the priority level of user, use the following command.

Command	Mode	Description
login tacacs priority-level {min user max root}	Global	Defines the priority level of user, refer the below information for the order of priority.



The order of priority is **root = max > user > min**.

4.2.6 Accounting Mode

The hiD 6610 S311 provides the accounting function of AAA (Authentication, Authorization, and Accounting). Accounting is the process of measuring the resources a user has consumed. Typically, accounting measures the amount of system time a user has used or the amount of data a user has sent and received.

To set an accounting mode, use the following command.

Command	Mode	Description
login accounting-mode {none start stop both}	Global	Sets an accounting mode. none: disables an accounting function. start: measures start point only. stop: measures stop point only. both: measures start and stop point both.

4.2.7 Displaying System Authentication

To display a configured system authentication, use the following command.

Command	Mode	Description
show login	Enable Global	Shows a configured system authentication.

4.3 Assigning IP Address

The switch uses only the data's MAC address to determine where traffic needs to come from and which ports should receive the data. Switches do not need IP addresses to transmit packets. However, if you want to access to the hiD 6610 S311 from remote place with TCP/IP through SNMP or telnet, it requires IP address.

You can enable interface to communicate with switch interface on network and assign IP address as the following:

- Enabling Interface
- Disabling Interface
- Assigning IP Address to Network Interface
- Static Route and Default Gateway
- Displaying Interface

4.3.1 Enabling Interface

To assign an IP address to an interface, you need to enable the interface first. If the interface is not enabled, you cannot access it from a remote place, even though an IP address has been assigned.

To display if interface is enabled, use the command, **show running-config**.

There are two ways to enable interface; on *Global Configuration* mode and on *Interface Configuration* mode.

Global Configuration Mode

To enable interface on *Global Configuration* mode, use the following command.

Command	Mode	Description
interface noshutdown <i>INTERFACE</i>	Global	Enables the interface on <i>Global Configuration</i> mode.



For multiple interfaces, use “-“ or “,” at *INTERFACES*.

Interface Configuration Mode

To open *Interface Configuration* mode of the interface you are about to enable interface, use the following command.

Command	Mode	Description
interface <i>INTERFACE</i>	Global	Opens <i>Interface Configuration</i> mode of the interface.

To enable the interface, use the following command.

Command	Mode	Description
no shutdown	Interface	Enables the interface on <i>Interface Configuration</i> mode.

The following is an example of enabling interface on *Global Configuration* mode or *Interface Configuration* mode.

```
SWITCH# configure terminal
SWITCH(config)# interface noshutdown 1
SWITCH(config)#

SWITCH# configure terminal
SWITCH(config)# interface 1
SWITCH(config-if)# no shutdown
SWITCH(config-if)#
```

4.3.2 Disabling Interface

To disable the interface, use the following commands on each mode.

Global Configuration Mode

To disable interface on Global Configuration mode, use the following command.

Command	Mode	Description
interface shutdown <i>INTERFACE</i>	Global	Disables a specified interface on <i>Global Configuration</i> mode.

Interface Configuration Mode

You also can disable interface on *Interface Configuration* mode. Before disabling interface on *Interface Configuration* mode, you should open the mode, and then use the follow command.

Command	Mode	Description
shutdown	Interface	Disables an interface on <i>Interface Configuration</i> mode.

4.3.3 Assigning IP Address to Network Interface

After enabling interface, you need to assign IP address. To assign IP address to specified network interface, use the following command.

Command	Mode	Description
ip address <i>IP-ADDRESS/M</i>	Interface	Assigns IP address to an interface.
ip address <i>IP-ADDRESS/M secondary</i>		Assigns secondary IP address to an interface.

To disable the assigned IP address, use the following command.

Command	Mode	Description
no ip address <i>IP-ADDRESS/M</i>	Interface	Removes assigned IP address to an interface.
no ip address <i>IP-ADDRESS/M secondary</i>		Removes assigned secondary IP address to an interface.

To display an assigned IP address, use the following command.

Command	Mode	Description
show ip	Interface	Shows an assigned IP address of the interface.

4.3.4 Static Route and Default Gateway

It is possible to configure the static route. Static route is a route which user configures manually. Packets are transmitted to the destination through static route. Static route includes destination address, neighbor router to receive packet, the number of routes that packets have to go through.

To configure static route, use the following command.

Command	Mode	Description
ip route <i>A.B.C.D SUBNET-MASK</i> { <i>GATEWAY</i> <i>null</i> } [<i><1-255></i>]	Global	Configures static route. A.B.C.D: destination IP prefix GATEWAY: Ip gateway address 1-255: Distance value
ip route <i>A.B.C.D/M</i> { <i>SUBNET-MASK</i> <i>null</i> } [<i><1-255></i> <i>src IP-ADDRESS</i>]		
no ip route <i>A.B.C.D SUBNET-MASK</i> { <i>GATEWAY</i> <i>null</i> } [<i><1-255></i>]		
no ip route <i>IP-ADDRESS/M</i> { <i>SUBNET-MASK</i> <i>null</i> } [<i><1-255></i>]		Deletes configured static route.

To configure default gateway, use the following command on *Global Configuration* mode.

Command	Mode	Description
ip route default { <i>GATEWAY</i> <i>null</i> } [<i><1-255></i>]	Global	Configures default gateway. GATEWAY: Ip gateway address
no ip route default { <i>GATEWAY</i> <i>null</i> } [<i><1-255></i>]		Deletes default gateway.

The following is an example of configuring static route to reach three destinations, which are not directly connected.

```
SWITCH(config)# ip route 100.1.1.0/24 10.1.1.2
SWITCH(config)# ip route 200.1.1.0/24 20.1.1.2
SWITCH(config)# ip route 172.16.1.0/24 30.1.1.2
```

To display configured static route, use the following command.

Command	Mode	Description
show ip route { <i>A.B.C.D</i> <i>A.B.C.D/M</i> summary static }	Enable	Shows configured routing information.
show ip route database static	Global	

4.3.5 Displaying Interface

To display interface status and configuration, use the following command.

Command	Mode	Description
show interface [INTERFACE]	Enable Global Interface	Shows interface status and configuration. INTERFACE: interface name
show ip interface [INTERFACE] brief	Enable Global	Shows brief information of interface. INTERFACE: interface name

4.4 SSH (Secure Shell)

Network security is getting more important according to using network has been generalized between users. However, typical FTP and telnet service has weakness for security. SSH (Secure Shell) is security shell for login. Through SSH, all data are encoded, traffic is compressed. So, transmit rate becomes faster, and tunnel for existing ftp and pop, which are not safe in security, is supported.

4.4.1 SSH Server

The hiD 6610 S311 can be operated as SSH server. You can configure the switch as SSH server with the following procedure.

- Enabling SSH Server
- Displaying On-line SSH Client
- Disconnecting SSH Client
- Displaying Connection History of SSH Client

4.4.1.1 Enabling SSH Server

To enable/disable SSH server, use the following command.

Command	Mode	Description
ssh server enable	Global	Enables SSH server.
ssh server disable		Disables SSH server.

4.4.1.2 Displaying On-line SSH Client

To display SSH clients connected to SSH server, use the following command.

Command	Mode	Description
show ssh	Enable/Global	Shows SSH clients connected to SSH server.

4.4.1.3 Disconnecting SSH Client

To disconnect an SSH client connected to SSH server, use the following command.

Command	Mode	Description
ssh disconnect <i>PID</i>	Global	Disconnects SSH clients connected to SSH server. PID: SSH client number

4.4.1.4 Displaying Connection History of SSH Client

To display the connection history of SSH client, use the following command.

Command	Mode	Description
ssh debug	Enable Global	Shows the connection history of SSH clients who are connected to SSH server up to now.

4.4.2 SSH Client

The hiD 6610 S311 can be used as SSH client with the following procedure.

- Login to SSH Server
- File Copy
- Configuring Authentication Key

4.4.2.1 Login to SSH Server

To login to SSH server after configuring the hiD 6610 S311 as SSH client, use the following command.

Command	Mode	Description
ssh login <i>DESTINATION</i>	Enable	Logins to SSH server. DESTINATION: IP address of SSH server or hostname and account

4.4.2.2 File Copy

To copy a file from/to SSH server, use the following command.

Command	Mode	Description
ssh copy <i>SOURCE DESTINATION</i>	Enable Global	Downloads or uploads a file to through SSH server. SOURCE: source file DESTINATION: destination file

4.4.2.3 Getting access to FTP

To use for securely getting access to a FTP service through SSH, use the following command.

Command	Mode	Description
ssh ftp <i>DESTINATION</i>	Enable Global	Access to FTP through SSH server. DESTINATION: FTP address

4.4.2.4 Configuring Authentication Key

SSH client can access to server through authentication key after configuring authentication key and informing it to server. It is safer to use authentication key than inputting password every time for login, and it is also possible to connect to several SSH servers with using one authentication key.

To configure authentication key in the hiD 6610 S311, use the following command.

Command	Mode	Description
ssh keygen {rsa1 rsa dsa}	Global	Configures authentication key. rsa1: SSH ver. 1 public key for the authentication rsa: SSH ver. 2 public key for the authentication dsa: SSH ver. 2 public key for the authentication

To configure authentication key and connect to SSH server with the authentication key, perform the following procedure.

Step 1

Configure the authentication key in the switch.

```
SWITCH_A(config)# ssh keygen dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/etc/.ssh/id_dsa):
Enter passphrase (empty for no passphrase): networks
Enter same passphrase again: networks
Your identification has been saved in /etc/.ssh/id_dsa.
Your public key has been saved in /etc/.ssh/id_dsa.pub.
The key fingerprint is:
d9:26:8e:3d:fa:06:31:95:f8:fe:f6:59:24:42:47:7e root@hiD6610
SWITCH_A(config)#
```

Step 2

Copy the generated authentication key to SSH server.

Step 3

Connect to SSH server with the authentication key.

```
SWITCH_A(config)# ssh login 172.16.209.10
Enter passphrase for key '/etc/.ssh/id_dsa': networks
SWITCH_B#
```

4.5 802.1x Authentication

To enhance security and portability of network management, there are two ways of authentication based on MAC address and port-based authentication which restrict clients attempting to access to port. The port-based authentication (802.1x) decides to give access to RADIUS server having the information about user who tries to access.

802.1x authentication adopts EAP (Extensible Authentication Protocol) structure. In EAP system, there are EAP-MD5 (Message Digest 5), EAP-TLS (Transport Level Security), EAP-SRP (Secure Remote Password), EAP-TTLS(Tunneled TLS) and the hiD 6610 S311 supports EAP-MD5 and EAP-TLS. Accessing with user's ID and password, EAP-MD5 is one-way Authentication based on the password. EAP-TLS accesses through the mutual authentication system of server authentication and personal authentication and it is possible to guarantee high security because of mutual authentication system.

At a request of user Authentication, from user's PC EAPOL-Start type of packets are transmitted to authenticator and authenticator again requests identification. After getting respond about identification, request to approve access to RADIUS server and be authenticated by checking access through user's information.

The following figure explains the process of 802.1x authentication.

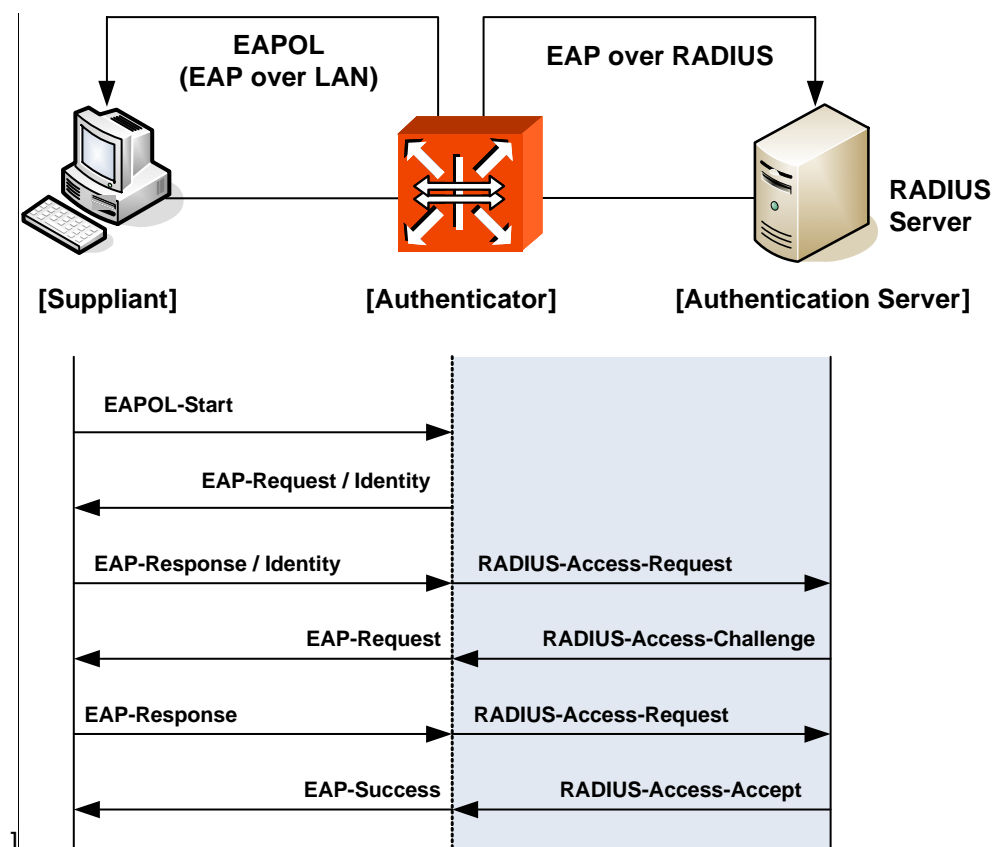


Fig. 4.1 Process of 802.1x Authentication

To enable 802.1x authentication on port of the hiD 6610 S311, you should be able to perform the following tasks.

4.5.1 802.1x Authentication

4.5.1.1 Enabling 802.1x

To configure 802.1x, the user should enable 802.1x daemon first. In order to enable 802.1x daemon, use the following command.

Command	Mode	Description
<code>dot1x system-auth-control</code>	Global	Enables 802.1x daemon.
<code>no dot1x system-auth-control</code>		Disables 802.1x daemon.

4.5.1.2 Configuring RADIUS Server

As RADIUS server is registered in authenticator, authenticator also can be registered in RADIUS server.

Here, authenticator and RADIUS server need extra data authenticating each other besides they register each other's IP address. The data is the key and should be the same value for each other. For the key value, every kinds of character can be used except for the space or special character.

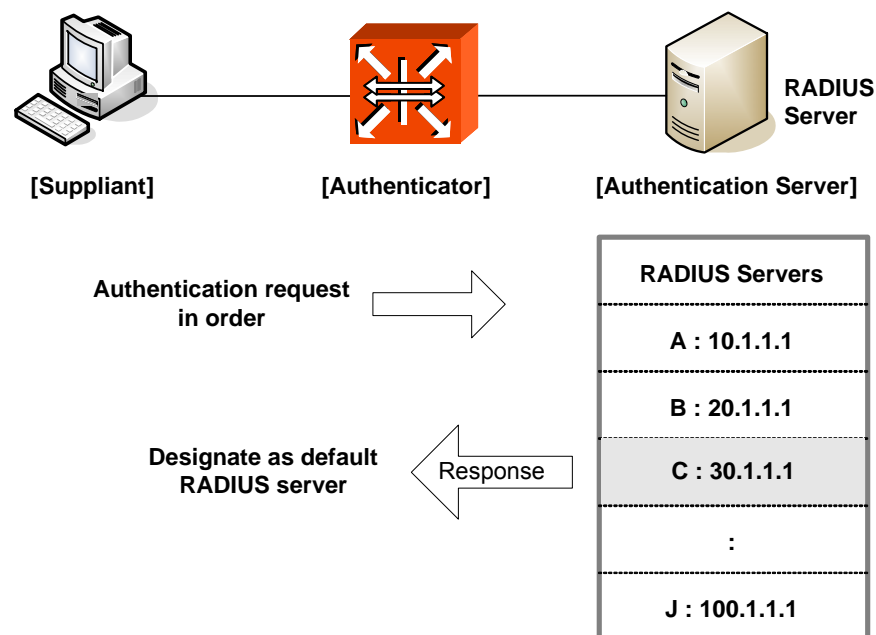


Fig. 4.2 Multiple Authentication Servers

If you register in several servers, the authentication server starts from RADIUS server registered as first one, then requests the second RADIUS server in case there's no response. According to the order of registering the authentication request, the authentication request is tried and the server which responds to it becomes the default server from the point of response time.

After default server is designated, all requests start from the RADIUS server. If there's no response from default server again, the authentication request is tried for RADIUS server designated as next one.

To configure IP address of RADIUS server and key value, use the following command.

Command	Mode	Description
dot1x radius-server host {IP-ADDRESS NAME} auth-port <0-65535> key KEY	Global	Registers RADIUS server with key value and UDP port of radius server. IP-ADDRESS: Ip address of radius server NAME: host name 0-65535: UDP port number KEY: the value of key
dot1x radius-server host {IP-ADDRESS NAME} key KEY		Configures IP address of RADIUS server and key value.
no dot1x radius-server host {IP-ADDRESS NAME}		Deletes a registered RADIUS server.



You can designate up to 5 RADIUS servers as authenticator.

The key is authentication information between the authenticator and RADIUS server. The authenticator and RADIUS server must have a same key value, and you can use alphabetic characters and numbers for the key value. The space or special character is not allowed.

You can configure the priority for the radius server that have configured by user.

Command	Mode	Description
dot1x radius-server move {IP-ADDRESS NAME} priority PRIORITY	Global	Configures the priority of radius server. IP-ADDRESS: Ip address of radius server NAME: host name

4.5.1.3 Configuring Authentication Mode

You can change the authentication mode from the port-based to the MAC-based. To change the authentication mode, use the following command.

Command	Mode	Description
dot1x auth-mode mac-base PORTS	Global	Sets the authentication mode to the MAC-based.
no dot1x auth-mode mac-base PORTS		Restores the authentication mode to the port-based.



Before setting the authentication mode to the MAC-based, you need to set a MAC filtering policy to deny them for all the Ethernet ports. To configure a MAC filtering policy, see Section 7.12.1

4.5.1.4 Authentication Port

After configuring 802.1x authentication mode, you should select the authentication port.

Command	Mode	Description
dot1x nas-port <i>PORTS</i>	Global	Designates 802.1x authentication port.
no dot1x nas-port <i>PORTS</i>		Disables 802.1x authentication port.

4.5.1.5 Force Authorization

The hiD 6610 S311 can allow the users to request the access regardless of the authentication from RADIUS server. For example, it is possible to configure not to be authenticated from the server even though a client is authenticated from the server.

To manage the approval for the designated port, use the following command.

Command	Mode	Description
dot1x port-control { <i>auto</i> <i>force-authorized</i> <i>force-unauthorized</i> } <i>PORTS</i>	Global	Configures the way of authorization to control port whether it has the RADIUS authentication or not.
no dot1x port-control <i>PORTS</i>		Deletes the configuration of the way of authorization to control port.

- **auto:** Follows the authentication of RADIUS server.
- **force-authorized:** Gives the authorization to a client even though RADIUS server didn't approve it.
- **force-unauthorized:** Don't give the authorization to a client even though RADIUS server authenticates it.

4.5.1.6 Configuring Interval for Retransmitting Request/Identity Packet

In hiD 6610 S311, it is possible to specify how long the device waits for a client to send back a response/identity packet after the device has sent a request/identity packet. If the client does not send back a response/identity packet during this time, the device retransmits the request/identity packet.

To configure the number of seconds that the switch waits for a response to a request/identity packet, use the following command.

Command	Mode	Description
dot1x timeout tx-period <1-65535> <i>PORTS</i>	Global	Sets reattempt interval for requesting request/identity packet. 1-65535: retransmit interval (default: 30)
no dot1x timeout tx-period <i>PORTS</i>		Disables the interval for requesting identity.

4.5.1.7 Configuring Number of Request to RADIUS Server

After 802.1x authentication configured as explained above and the user tries to connect with the port, the process of authentication is progressed among user's PC and the equipment as authenticator and RADIUS server. It is possible to configure how many times the device which will be authenticator requests for authentication to RADIUS server.

To configure times of authentication request in the hiD 6610 S311, please use the command in *Global Configuration* mode.

Command	Mode	Description
dot1x radius-server retries <1-10>	Global	Configure times of authentication request to RADIUS server. 1-10: retry number

4.5.1.8 Configuring Interval of Request to RADIUS Server

For the hiD 6610 S311, it is possible to set the time for the retransmission of packets to check RADIUS server. If there's a response from other packets, the switch waits for a response from RADIUS server during the configured time before resending the request.

To set the interval of request to RADIUS server, use the following command.

Command	Mode	Description
dot1x radius-server timeout <1-120>	Global	Configures the interval of request to RADIUS server. 1-120: 1-120 seconds (Default value: 1)

You should consider the distance from the server for configuring the interval of requesting the authentication to RADIUS server. If you configure the interval too short, the authentication couldn't be realized. If it happens, you'd better to reconfigure the interval longer.

4.5.2 802.1x Re-Authentication

In hiD 6610 S311, it is possible to update the authentication status on the port periodically. To enable re-authentication on the port, you should perform the below procedure.

Step 1

Enable 802.1x re-authentication

Step 2

Configure the interval of re-authentication

Step 3

Configuring the interval of requesting re-authentication in case of re-authentication fails.

Step 4

Executing 802.1x re-authenticating regardless of the interval

4.5.2.1 Enabling 802.1x Re-Authentication

To enable 802.1x re-authentication using the following command.

Command	Mode	Description
dot1x reauth-enable <i>PORTS</i>	Global	Enables 802.1x re-authentication.
no dot1x reauth-enable <i>PORTS</i>		Disables 802.1x re-authentication.

4.5.2.2 Configuring the Interval of Re-Authentication

RADIUS server contains the database about the user who has access right. The database is real-time upgraded so it is possible for user to lose the access right by updated database even though he is once authenticated. In this case, even though the user is accessible to network, he should be authenticated once again so that the changed database is applied to. Besides, because of various reasons for managing RADIUS server and 802.1x authentication port, the user is supposed to be re-authenticated every regular time. The administrator of hiD 6610 S311 can configure a term of re-authentication.

To configure a term of re-authentication, use the following command.

Command	Mode	Description
dot1x timeout reauth-period <1-4294967295> <i>PORTS</i>	Global	Sets the period between re-authentication attempts.
no dot1x timeout reauth-period <i>PORTS</i>		Deletes the period between re-authentication attempts.

4.5.2.3 Configuring the Interval of Requesting Re-authentication

When the authenticator sends Request/Identity packet for re-authentication and no response is received from the suppliant for the number of seconds, the authenticator retransmits the request to the suppliant. In hiD 6610 S311, you can set the number of seconds that the authenticator should wait for a response to request/identity packet from the suppliant before retransmitting the request.

To set a period that the authenticator waits for a response, use the following command.

Command	Mode	Description
dot1x timeout quiet-period <1-65535> <i>PORTS</i>	Global	Sets reattempt interval for requesting request/identity packet. 1-65535: reattempt interval seconds PORTS: enters port number
no dot1x timeout quiet-period <i>PORTS</i>		Disables the interval for requesting identity.

4.5.2.4 802.1x Re-authentication

In 4.5.2.2 Configuring the Interval of Re-Authentication, it is described even though the user is accessible to network, he should be authenticated so that the changed database is applied to.

Besides, because of various reasons managing RADIUS server and 802.1x authentication port, the user is supposed to be re-authenticated every regular time.

To implement re-authentication immediately regardless of configured time interval, user the following command.

Command	Mode	Description
dot1x reauthenticate <i>PORTS</i>	Global	Implement re-authentication regardless of the configured time interval.

4.5.3 Initializing Authentication Status

The user can initialize the entire configuration on the port. Once the port is initialized, the supplicants accessing to the port should be re-authenticated.

Command	Mode	Description
dot1x initialize <i>PORTS</i>	Global	Initializes the authentication status on the port.

4.5.4 Applying Default Value

To apply the default value to the system, use the following command.

Command	Mode	Description
dot1x default <i>PORTS</i>	Global	Applies the default value.

4.5.5 Displaying 802.1x Configuration

To display 802.1x configuration, use the following command.

Command	Mode	Description
show dot1x [<i>PORTS</i>]	Enable Global	Shows 802.1x configuration.

4.5.6 802.1x User Authentication Statistic

To display the statistics about the process of 802.1x user authentication, use the following command.

Command	Mode	Description
show dot1x statistics <i>PORTS</i>	Global	Shows the statistics of 802.1x user authentication on the port.

To reset statistics by deleting the statistics of 802.1x user authentication, use the following command.

Command	Mode	Description
dot1x clear statistics <i>PORTS</i>	Global	Makes reset state by deleting the statistics of 802.1x on the port.

4.5.7 Sample Configuration

The following is to show the configuration after configuring port number 4 as the authentication port and registering IP address of authentication port and information of RADIUS server.

```
SWTICH(config)# dot1x system-auth-control
SWTICH(config)# dot1x nas-port 4
SWTICH(config)# dot1x port-control force-authorized 4
SWTICH(config)# dot1x radius-server host 10.1.1.1 auth-port 4 key test
SWTICH(config)# show dot1x
802.1x authentication is enabled.
RADIUS Server : 10.1.1.1 (Auth key : test)
-----
          |           1           2           3           4
802.1x    |123456789012345678901234567890123456789012
-----
PortEnable |...p.....
PortAuthed |...u.....
MacEnable  |.....
MacAuthed  |.....
-----
p = port-based, m = mac-based, a = authenticated, u = unauthenticated

SWTICH(config)#
```

The following is configuring a term of re-authentication as 1800 and a term of re-authentication as 1000 sec.

```
SWTICH(config)# dot1x timeout quiet-period 1000 4
SWTICH(config)# dot1x timeout reauth-period 1800 4
SWTICH(config)# dot1x reauth-enable 4
SWTICH(config)# show dot1x 4
Port 4
  SystemAuthControl : Enabled
  ProtocolVersion   : 0
  PortControl       : Force-Authorized
  PortStatus        : Unauthorized
  ReauthEnabled     : True
  QuietPeriod       : 1000
  ReauthPeriod      : 1800
SWTICH(config)#
```

The following is an example of showing the configuration after configuring the authentication based on MAC address.

```
SWTICH(config)# dot1x auth-mode mac-base 4
SWTICH(config)# show dot1x
802.1x authentication is enabled.
RADIUS Server : 10.1.1.1 (Auth key : test)
-----
          |           1           2           3           4
802.1x    |123456789012345678901234567890123456789012
-----
PortEnable |.....
PortAuthed |.....
MacEnable  |...m.....
MacAuthed  |...u.....
-----
p = port-based, m = mac-based, a = authenticated, u = unauthenticated

SWTICH(config)#
```

5 Port Configuration

It is possible for user to configure basic environment such as auto-negotiate, transmit rate, and flow control of the hiD 6610 S311 port. Also, it includes instructions how to configure port mirroring and port as basic.

5.1 Port Basic

It is possible to configure default environment of port such as port state, speed. To configure port, you need to open *Bridge Configuration* mode by using the command, **bridge**, on *Global Configuration* mode. When you begin *Bridge Configuration* mode, system prompt will be changed from SWITCH(config)# to SWITCH(bridge)#.

```
SWITCH(config)# bridge
SWITCH(bridge)#
```

The hiD 6610 S311 can have 24 ports of 10/100Base- TX Ethernet interfaces and 4 Giga-Ethernet uplink ports. The direction to configure each port is different depending on its features. Read the below instruction carefully and follow it before you configure.

Port Number

The hiD 6610 S311 has 1-24 ports of Fast Ethernet interface support 10/100Base-TX (RJ-45 type). 2 ports of 10/100/1000Base-TX have the port number of 25 to 26. 2 ports of 1000Base-X with SFP module have the port number of 27 and 28. These interfaces can be used as uplink towards the core network.

Refer to below figure for front interfaces of hiD 6610 S311.

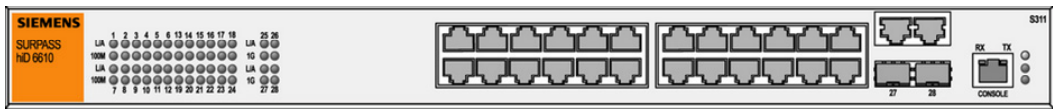


Fig. 5.1 hiD 6610 S311 Interface

To display the configuration of the physical port, use the following command.

Command	Mode	Description
show port [PORTS]	Enable Global Bridge	Shows port configuration.

When you use the command, show port command, if you input letter at port-number, the message, “% Invalid port: port” will be displayed, and if you input wrong number, the message, “% Invalid range: 100 [1-42]” will be displayed.

```
SWITCH(bridge)# show port port
%Invalid port: port
SWITCH(bridge)# show port 100
%Invalid range: 100 [1-42]
SWITCH(bridge)#
```


5.2 Ethernet Port Configuration

5.2.1 Enabling Ethernet Port

To enable/disable a port, use the following command.

Command	Mode	Description
port {enable disable} PORTS	Bridge	Enables/disables a port, enter a port number. (Default: enable)

The following is an example of disabling the Ethernet port 1 to 3.

```
SWITCH(config)# bridge
SWITCH(bridge)# show port 1-5
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
      (ADMIN/OPER)
-----
1: Ethernet      1      Up/Down  Auto/Half/0  Off      N
2: Ethernet      1      Up/Down  Auto/Half/0  Off      N
3: Ethernet      1      Up/Down  Auto/Half/0  Off      N
4: Ethernet      1      Up/Down  Auto/Half/0  Off      N
5: Ethernet      1      Up/Down  Auto/Half/0  Off      N
SWITCH(bridge)# port disable 1-3
SWITCH(bridge)# show port 1-5
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
      (ADMIN/OPER)
-----
1: Ethernet      1      Down/Down Auto/Half/0  Off      N
2: Ethernet      1      Down/Down Auto/Half/0  Off      N
3: Ethernet      1      Down/Down Auto/Half/0  Off      N
4: Ethernet      1      Up/Down  Auto/Half/0  Off      N
5: Ethernet      1      Up/Down  Auto/Half/0  Off      N
SWITCH(bridge)#
```

5.2.2 Auto-negotiation

Auto-negotiation is a mechanism that takes control of the cable when a connection is established to a network device. Auto-negotiation detects the various modes that exist in the network device on the other end of the wire and advertises its own abilities to automatically configure the highest performance mode of interoperation. As a standard technology, this allows simple, automatic connection of devices that support a variety of modes from a variety of manufacturers.

To enable/disable the auto-negotiation on an Ethernet port, use the following command.

Command	Mode	Description
port nego PORTS {on off}	Bridge	Configures the auto-negotiation of the specified port, enter the port number.

For the hiD 6610 S311, you can configure transmit rate and duplex mode as standard to configure transmit rate or duplex mode of connected equipment even when auto-negotiation is enabled. For example, when you configure transmit rate as 10Mbps with configured auto-negotiation, a port is worked by the standard 10Mbps/full duplex mode.



By default, auto-negotiation is activated in 10/100/1000Base-TX port of the hiD 6610 S311. However you cannot configure auto-nego in fiber port.

The following is an example of deleting auto-negotiate of port 7 and 8, and showing it.

```
SWITCH(bridge)#
SWITCH(bridge)# port nego 7-8 off
SWITCH(bridge)# show port 7-8
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
      (ADMIN/OPER)
-----
7:  Ethernet      7      Up/Up      Force/Full/100  Off      Y
8:  Ethernet      8      Up/Up      Force/Full/100  Off      Y
SWITCH(bridge)#
```

5.2.3 Transmit Rate

To set transmit rate of Ethernet port, use the following command.

Command	Mode	Description
port speed <i>PORTS</i> {10 100 1000}	Bridge	Sets transmit rate of Ethernet port as 10/100/1000Mbps, enter the port number.



When auto-nego is activated, it is impossible to change transmit rate.

5.2.4 Duplex Mode

Only unidirectional communication is practicable on half duplex mode, and bidirectional communication is practicable on full duplex mode. By transmitting packet for two ways, Ethernet bandwidth is enlarged two times- 10Mbps to 20Mbps, 100Mbps to 200Mbps.

To set duplex mode, use the following command.

Command	Mode	Description
port duplex <i>PORTS</i> {full half}	Bridge	Sets full or half duplex mode of specified port, enter the port number.

The following is an example of configuring duplex mode of port 1 as half mode and showing it.

```
SWITCH(bridge)# show port 1
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
      (ADMIN/OPER)
-----
1: Ethernet      1      Up/Up      Force Full/100      Off      Y
SWITCH(bridge)# port duplex 1 half
SWITCH(bridge)# show port 1
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
      (ADMIN/OPER)
-----
1: Ethernet      1      Up/Down    Force Half/100      Off      Y
SWITCH(bridge)#
```

5.2.5 Flow Control

Ethernet ports on the switches use flow control to restrain the transmission of packets to the port for a period time. Typically, if the receive buffer becomes full, the port transmits a pause packet that tells remote ports to delay sending more packets for a specified period time. In addition, the Ethernet ports can receive and act upon pause packets from other devices.

To configure flow control of the Ethernet port, use the following command.

Command	Mode	Description
port flow-control <i>PORTS</i> {on off}	Bridge	Configures flow control for a specified port, enter the port number. (default: off)

The following is an example of configuring flow control to port 4.

```
SWITCH(bridge)# show port 25
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
      (ADMIN/OPER)
-----
25 Ethernet      1      Up/Down    Auto/Half/0 Off      Y
SWITCH(bridge)# port flow-control 25 on
SWITCH(bridge)# show port 25
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
      (ADMIN/OPER)
-----
25: Ethernet      1      Up/Down    Auto/Half/0 On      Y
SWITCH(bridge)#
```

5.2.6 Port Description

To specify a description of an Ethernet port, use the following command.

Command	Mode	Description
port description <i>PORTS</i> <i>DESCRIPTION</i>	Bridge	Specifies a description of an Ethernet port.

5.2.7 Traffic Statistics

To display traffic statistic of each port or interface with MIB or RMON MIB data defined, use the following commands.

Command	Mode	Description
show port statistics avg-pkt [<i>PORTS</i>]	Enable Global Bridge	Shows traffic average of specified port, enter port number.
show port statistics avg-pps [<i>PORTS</i>]		Shows Unicast, Multicast and Broadcast traffic average of specified port.
show port statistics interface [<i>PORTS</i>]		Shows MIB data of specified port.
show port statistics rmon [<i>PORTS</i>]		Shows RMON statistic counters of specified port, enter the port number.

The following is an example of displaying traffic average of port 1.

```
SWITCH(bridge)# show port statistics avg-pkt 1
=====
Slot/Port |          Tx          |          Rx          |
-----|-----|-----|-----|-----|
Time | pkts/s | bits/s | pkts/s | bits/s |
-----|-----|-----|-----|-----|
port 1 -----
5 sec:      1      608      120      61,848
1 min:      3     3,242     122     62,240
10 min:     0      440      39     20,272
SWITCH(bridge)#
```

The following is an example of displaying RMON statistic counters of port 1.

```
SWITCH(bridge)# show port statistics rmon 1
Port1

EtherStatsDropEvents          0
EtherStatsOctets              5,669,264
EtherStatsPkts                71,811
EtherStatsBroadcastPkts       36,368
EtherStatsMulticastPkts       32,916
EtherStatsCRCAlignErrors      0
EtherStatsUndersizePkts       0
EtherStatsOversizePkts        0
EtherStatsFragments           0
EtherStatsJabbers             0
EtherStatsCollisions          0
```

```

EtherStatsPkts64Octets          165,438
EtherStatsPkts65to127Octets     12,949
EtherStatsPkts128to255Octets    1,662
EtherStatsPkts256to511Octets    31,177
EtherStatsPkts512to1023Octets   12
EtherStatsPkts1024to1518Octets  64
SWITCH(bridge)#

```

Otherwise, to clear all recorded statistics of port and initiate, use the following command.

Command	Mode	Description
clear port statistics { <i>PORTS</i> all }	Enable Global Bridge	Clears all recorded port statistics.

5.2.8 Port Status

To display a port status, use the following command.

Command	Mode	Description
show port <i>PORTS</i>	Enable Global Bridge	Shows configured state of port, enter the port number.
show port <i>PORTS</i> description [<i>PORTS</i>]		Shows port specific description (max. number of characters is 100), enter the port number.
show port module-info [<i>PORTS</i>]		Shows port module information.

5.3 Port Mirroring

Port mirroring is the function of monitoring a designated port. Here, one port to monitor is called monitor port and a port to be monitored is called mirrored port. Traffic transmitted from mirrored port is sent to monitor port so that user can monitor network traffic.

The following is a network structure to analyze the traffic by port mirroring. It analyzes traffic on the switch and network status by configuring Mirrored port and Monitor port connecting the computer, that the watch program is installed, to the port configured as Monitor port.

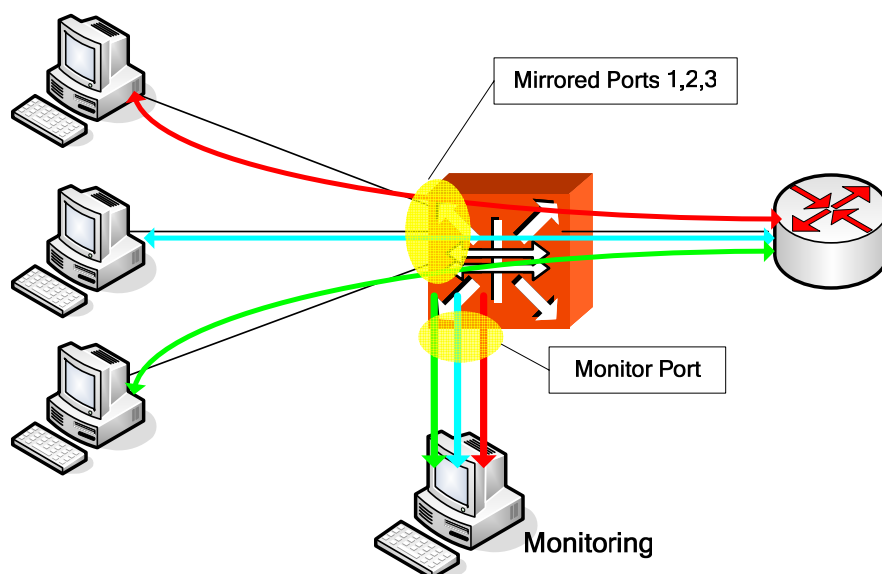


Fig. 5.2 Port Mirroring

To configure port mirroring, designate mirrored ports and monitor port. Then enable port mirroring function. Monitor port should be connected to the watch program installed PC. You can designate only one monitor port but many mirrored ports for one switch.

Step 1

Activate the port mirroring, using the following command.

Command	Mode	Description
mirror enable	Bridge	Activates port mirroring.

Step 2

Designate the monitor port, use the following command.

Command	Mode	Description
mirror monitor {PORTS cpu}	Bridge	Designates the monitor port.

Step 3

Designate the mirrored ports, use the following command.

Command	Mode	Description
mirror add PORTS [ingress egress]	Bridge	Designates the mirrored ports. ingress: ingress traffic egress: egress traffic

Step 4

To delete and modify the configuration, use the following command.

Command	Mode	Description
mirror disable	Bridge	Deactivate monitoring.
mirror del PORTS [ingress egress]		Delete a port from the mirrored ports.

Step 5

To disable monitoring function, use the following command.

Command	Mode	Description
no mirror monitor	Bridge	Disable port mirroring function.

The following is an example of configuring port mirroring with a port.

Step 1

Connect a motoring PC to the monitor port of the switch.

Step 2

Enable mirroring function.

```
SWITCH(bridge)# mirror enable
SWITCH(bridge)#
```

Step 3

Configure the monitor port 1 and mirroring port 2, 3, 4 and 5.

```
SWITCH(bridge)# mirror monitor 1
SWITCH(bridge)# mirror add 2
SWITCH(bridge)# mirror add 3-5
SWITCH(bridge)#
```

Step 4

Check the configuration.

```
SWITCH(bridge)# show mirror
Mirroring enabled
Monitor port = 1

Ingress mirrored ports
-- 02 03 04 05 -- -- -- -- -- -- -- -- -- --
Egress mirrored ports
-- 02 03 04 05 -- -- -- -- -- -- -- -- -- --
SWITCH(bridge)#
```

6 System Environment

6.1 Environment Configuration

You can configure a system environment of the hiD 6610 S311 with the following items:

- Host Name
- Time and Date
- Time Zone
- Network Time Protocol
- Simple Network Time Protocol (SNTP)
- Terminal Configuration
- Login Banner
- DNS Server
- Fan Operation
- Disabling Daemon Operation
- System Threshold

6.1.1 Host Name

Host name displayed on prompt is necessary to distinguish each device connected to network.

To set a new host name, use the following command.

Command	Mode	Description
hostname <i>NAME</i>	Global	Creates a host name of the switch, enter the name.
no hostname [<i>NAME</i>]		Deletes a configured host name, enter the name.

To see a new host name, use the following command.

Command	Mode	Description
show running-config hostname	Global	Shows the host name.

6.1.2 Time and Date

To set system time and date, use the following command.

Command	Mode	Description
clock <i>DATETIME</i>	Enable	Sets system time and date.
show clock	Global	Shows system time and date.

The following is an example of setting system time and date as 10:20pm, July 4th, 2005.

```
SWITCH# clock 06 Mar 2006 10:20
Mon, 6 Mar 2006 10:20:00 GMT+0000
SWITCH#
```


6.1.3 Time Zone

The hiD 6610 S311 provides three kinds of time zone, GMT, UCT and UTC. The time zone of the switch is predefined as GMT (Greenwich Mean Time). Also you can set the time zone where the network element belongs.

To set the time zone, use the following command (Refer to the below table).

Command	Mode	Description
time-zone <i>TIMEZONE</i>	Global	Sets the time zone.
show time-zone	Enable Global	Shows the world time zone map.

Tab. 6.1 shows the world time zone.

Time Zone	Country/City	Time Zone	Country/City	Time Zone	Country/City
GMT-12	Eniwetok	GMT-3	Rio De Janeiro	GMT+6	Rangoon
GMT-11	Samoa	GMT-2	Maryland	GMT+7	Singapore
GMT-10	Hawaii, Honolulu	GMT-1	Azores	GMT+8	Hong Kong
GMT-9	Alaska	GMT+0	London, Lisbon	GMT+9	Seoul, Tokyo
GMT-8	LA, Seattle	GMT+1	Berlin, Rome	GMT+10	Sydney,
GMT-7	Denver	GMT+2	Cairo, Athens	GMT+11	Okhotsk
GMT-6	Chicago, Dallas	GMT+3	Moscow	GMT+12	Wellington
GMT-5	New York, Miami	GMT+4	Teheran		
GMT-4	George Town	GMT+5	New Dehli		

Tab. 6.1 World Time Zone

6.1.4 Network Time Protocol

The Network Time Protocol (NTP) provides a mechanism to synchronize time on computers across an internet. The specification for NTP is defined in RFC 1119.

To enable/disable the NTP function, use the following command.

Command	Mode	Description
ntp <i>SERVER1</i> <i>[[SERVER2]</i> <i>SERVER3]]</i>	Global	Enables the NTP function with specified NTP server. SERVER: server IP address
ntp start		Operates the NTP function with specified NTP server.
no ntp		Disables the NTP function.

To display a configured NTP, use the following command.

Command	Mode	Description
show ntp	Enable Global	Shows a configured NTP function.

6.1.5 Simple Network Time Protocol (SNTP)

NTP (Network Time Protocol) and SNTP (Simple Network Time Protocol) are the same TCP/IP protocol in that they use the same UDP time packet from the Ethernet Time Server message to compute accurate time. The basic difference in the two protocols is the algorithms being used by the client in the client/server relationship.

The NTP algorithm is much more complicated than the SNTP algorithm. NTP normally uses multiple time servers to verify the time and then controls the rate of adjustment or slew rate of the PC which provides a very high degree of accuracy. The algorithm determines if the values are accurate by identifying time server that doesn't agree with other time servers. It then speeds up or slows down the PC's drift rate so that the PC's time is always correct and there won't be any subsequent time jumps after the initial correction. Unlike NTP, SNTP usually uses just one Ethernet Time Server to calculate the time and then it "jumps" the system time to the calculated time. It can, however, have back-up Ethernet Time Servers in case one is not available.

To configure the switch in SNTP, use the following commands.

Command	Mode	Description
sntp SERVER 1 [SERVER 2] [SERVER 3]	Global	Specifies the IP address of the SNTP server. It is possible up to three number of server. SERVER: server IP address
sntp start		Enables SNTP function
no sntp		Disables SNTP function.

To display SNTP configuration, use the following command.

Command	Mode	Description
show sntp	Enable Global	Show SNTP configuration.

The following is to register SNTP server as 203.255.112.96 and enable it.

```
SWITCH(config)# sntp 203.255.112.96
SWITCH(config)# show sntp
=====
sntpd is running.
=====
Time Servers
-----
1st : 203.255.112.96
=====
SWITCH(config)#
```



You can configure up to 3 servers so that you use second and third servers as backup use in case the first server is down.

6.1.6 Terminal Configuration

By default, the hiD 6610 S311 is configured to display 24 lines composed by 80 characters on console terminal. The maximum line displaying is 512 lines.

To set the number of line displaying on terminal screen, use the following command.

Command	Mode	Description
terminal length <0-512>	Global	Sets the number of line displaying on console terminal, enter the value.
no terminal length		Restores a default line displaying.

6.1.7 Login Banner

It is possible to set system login and log-out banner. Administrator can leave a message to other users with this banner.

To set system login and log-out banner, use the following command.

Command	Mode	Description
banner	Global	Sets a banner before login the system.
banner login		Sets a banner when successfully log in the system.
banner login-fail		Sets a banner when failing to login the system.

To restore a default banner, use the following command.

Command	Mode	Description
no banner	Global	Restores a default banner.
no banner login		
no banner login-fail		

To display a current login banner, use the following command.

Command	Mode	Description
show banner	Enable Global	Shows a current login banner.

6.1.8 DNS Server

To set a DNS server, use the following command.

Command	Mode	Description
dns-server <i>A.B.C.D</i>	Global	Sets a DNS server.
no dns-server <i>A.B.C.D</i>		Removes a DNS server.
show dns	Enable Global	Shows a DNS server.

If a specific domain name is registered instead of IP address, user can do telnet, FTP, TFTP and ping command to the hosts on the domain with domain name.

To configure DNS domain name, use the following command.

Command	Mode	Description
dns search <i>DOMAIN</i>	Global	Searches a domain name.
no dns search <i>DOMAIN</i>		Removes a domain name.

It is possible to delete DNS server and domain name at the same time with the below command.

Command	Mode	Description
no dns	Global	Deletes DNS server and domain name.

6.1.9 Fan Operation

In hiD 6610 S311, it is possible to control fan operation. To control fan operation, use the following command.

Command	Mode	Description
fan operation {on off}	Global	Configures fan operation.

i

It is possible to configure to start and stop fan operation according to the system temperature. To configure this, refer the Section 6.1.11.3.

To display fan status and the temperature for fan operation, use the following command.

Command	Mode	Description
show status fan	Enable Global	Shows the fan status and the temperature for the fan operation.

6.1.10 Disabling Daemon Operation

You can disable the daemon operation unnecessarily occupying CPU. To disable certain daemon operation, use the following command.

Command	Mode	Description
halt <i>PID</i>	Enable	Disables the daemon operation.

You can display PID of daemon with the **show process** command.

```
SWITCH# show process
USER      PID  %CPU %MEM  VSZ  RSS  TTY      STAT START  TIME COMMAND
admin      1   0.0  0.5  1448  592  ?        S    15:56  0:03 init [3]
admin      2   0.0  0.0    0    0  ?        S    15:56  0:00 [keventd]
admin      3   0.0  0.0    0    0  ?        SN   15:56  0:00 [ksoftirqd_CPU0]
admin      4   0.0  0.0    0    0  ?        S    15:56  0:00 [kswapd]
--More--
```

6.1.11 System Threshold

You can configure the switch with various kinds of the system threshold like CPU load, traffic, temperature, etc. Using this threshold, the hiD 6610 S311 generates syslog messages, sends SNMP traps, or performs a related procedure.

6.1.11.1 CPU Load

To set a threshold of CPU load, use the following command.

Command	Mode	Description
threshold cpu <21-100> {5 60 600} [<20-100> {5 60 600}]	Global	Sets a threshold of CPU load in the unit of percent (%). 20-100: CPU load (default: 50) 5 60 600: time Interval (second)
no threshold cpu		Deletes a configured threshold of CPU load.

To show a configured threshold of CPU load, use the following command.

Command	Mode	Description
show cpuload	All	Shows a configured threshold of CPU load.

6.1.11.2 Port Traffic

To set a threshold of port traffic, use the following command.

Command	Mode	Description
threshold port <i>PORTS</i> <i>THRESHOLD</i> {5 60 600} {rx tx}	Global	Sets a threshold of port traffic. <i>PORTS</i> : port number (1/1, 1/2, 2/1, ...) <i>THRESHOLD</i> : threshold value (unit: kbps) 5 60 600: time Interval (unit: second)
no threshold port <i>PORTS</i> {rx tx}		Deletes a configured threshold of port traffic.



The threshold of the port is set to the maximum rate of the port as a default.

To show a configured threshold of port traffic, use the following command.

Command	Mode	Description
show port threshold	Enable Global	Shows a configured threshold of port traffic.

6.1.11.3 Fan Operation

The system fan will operate depending on a configured fan threshold. To set a threshold of port traffic, use the following command.

Command	Mode	Description
threshold fan <i>START-TEMP</i> <i>STOP-TEMP</i>	Global	Sets a threshold of fan operation in the unit of centigrade (°C). START-TEMP: starts fan operation. (default: 30) STOP-TEMP: stops fan operation. (default: 0)
no threshold fan		Deletes a configured threshold of fan operation.



When you set a threshold of fan operation, *START-TEMP* must be higher than *STOP-TEMP*.

To show a configured threshold of fan operation, use the following command.

Command	Mode	Description
show status fan	Enable /Global / Bridge	Shows a status and configured threshold of fan operation.

6.1.11.4 System Temperature

To set a threshold of system temperature, use the following command.

Command	Mode	Description
threshold temp <i>OVERLOAD</i> <i>UNDERLOAD</i>	Global	Sets a threshold of system temperature in the unit of centigrade (°C). OVERLOAD: Overload Threshold temperature between -40 ~100 (default: 80) UNDERLOAD: Underload Threshold temperature between -40 ~100
no threshold temp		Deletes a configured threshold of system temperature.

To show a configured threshold of system temperature, use the following command.

Command	Mode	Description
show status temp	Enable Global	Shows a status and configured threshold of system temperature.

6.1.11.5 System Memory

To set a threshold of system memory in use, use the following command.

Command	Mode	Description
threshold memory <20-100>	Global	Sets a threshold of system memory in the unit of percent (%). 20-100: system memory in use

6.2 Configuration Management

You can verify if the system configurations are correct and save them in the system. This section contains the following functions.

- Displaying System Configuration
- Saving System Configuration
- Auto-Saving
- System Configuration File
- Restoring Default Configuration

6.2.1 Displaying System Configuration

To display a current running configuration of the system, use the following command.

Command	Mode	Description
show running-config	All	Shows a configuration of the system.
show running-config {admin-rule arp bridge dns full hostname instance interface INTERFACE login pm qos rmon-alarm rmon-event rmon-history router {bgp pim rip ospf vrrp} rule snmp syslog time-out time-zone time-out}		Shows a configuration of the system with the specific option.

The following is an example to display a configuration of syslog.

```
SWITCH# show running-config syslog
!
syslog start
syslog output info local volatile
syslog output info local non-volatile
!
SWITCH#
```

6.2.2 Saving System Configuration

If you change a configuration of the system, you need to save the changes in the system flash memory.

To save all changes of the system, use the following command.

Command	Mode	Description
write memory	All	Saves all changes in the system flash memory.



When you use the command, **write memory**, make sure there is no key input until **[OK]** message appears.

6.2.3 Auto-Saving

In hiD 6610 S311, it is possible to save the configuration automatically. To configure the con-figuration periodically, use the following command.

Command	Mode	Description
write interval <10-1440>	Global	Saves auto-configuration periodically. 10-1440: auto-saving interval (unit: minute)
no write interval		Disables auto-saving function.

6.2.4 System Configuration File

To manage a system configuration file, use the following command.

Command	Mode	Description
copy running-config { <i>FILENAME</i> startup-config }	Enable	Copies a running configuration file. FILENAME: configuration file name startup-config: startup configuration file
copy startup-config <i>FILENAME</i>		Copies a startup configuration file. FILENAME: configuration file name.
copy <i>FILENAME</i> startup-config		Copies a specified configuration file to the startup configuration file. FILENAME: configuration file name
copy <i>FILENAME1</i> <i>FILENAME2</i>		Copies a specified configuration file to another configuration file.
erase <i>FILENAME</i>		Deletes a specified configuration file. FILENAME: configuration file name

To back up a system configuration file using FTP or TFTP, use the following command.

Command	Mode	Description
copy { ftp tftp } config upload { <i>FILE-NAME</i> startup-config }	Enable	Uploads a file to ftp or tftp server with a name configured by user.
copy { ftp tftp } config download { <i>FILE-NAME</i> startup-config }		Downloads a file from ftp or tftp server with a name configured by user.
copy { ftp tftp } os upload { os1 os2 }		Uploads a file to ftp or tftp server with a name of os1 or os2.
copy { ftp tftp } os download { os1 os2 }		Downloads a file from ftp or tftp server with a name of os1 or os2.



To access FTP to back up the configuration or use the backup file, you should know FTP user ID and the password. To back up the configuration or use the file through FTP, you can check the file transmission because hash function is automatically turned on.

To display a system configuration file, use the following command.

Command	Mode	Description
show startup-config	Enable	Shows a current startup configuration.
show config-list	Enable Global	Shows a list of configuration files.

The following is an example of displaying a list of configuration files.

```
SWITCH(config)# copy running-config SURPASShiD6610
SWITCH(config)# show config-list
=====
          CONFIG-LIST
=====
l3_default
SURPASShiD6610
SWITCH(config)#
```

6.2.5 Restoring Default Configuration

To restore a default configuration of the system, use the following command.

Command	Mode	Description
restore factory-defaults	Global	Restores a factory default configuration.
restore layer2-defaults		Restores an L2 default configuration.
restore layer3-defaults		Restores an L3 default configuration.



After restoring a default configuration, you need to restart the system to initiate.

The following is an example of restoring a default configuration of the system.

```
SWITCH(config)# restore factory-defaults
[OK]
SWITCH(config)#
```

6.3 System Management

When there is any problem in the system, you must find what the problem is and its solution. Therefore, you should not only be aware of a status of the system but also verify that the system is configured properly.

This section includes the following functions with CLI command.

- Network Connection
- IP ICMP Source-Routing
- Tracing Packet Route
- Displaying User Connecting to
- MAC Table
- Running Time of System
- System Information
- System Memory Information
- Average of CPU Load
- Running Process
- Displaying System Image
- Displaying Installed OS
- Default OS
- Switch Status
- Tech Support

6.3.1 Network Connection

To verify if your system is correctly connected to the network, use the command, **ping**. For IP network, this command transmits echo message to ICMP (Internet Control Message Protocol). ICMP is internet protocol that notifies fault situation and provides information on the location where IP packet is received. When ICMP echo message is received at the location, its replying message is returned to the place where it came.

To perform a ping test to verify network status, use the following command.

Command	Mode	Description
ping [IP-ADDRESS]	Enable	Performs a ping test to verify network status.

The following is the basic information to operate ping test.

Items	Description
Protocol [ip]	Supports ping test. Default is IP.
Target IP address	Sends ICMP echo message by inputting IP address or host name of destination in order to check network status with relative.
Repeat count [5]	Sends ICMP echo message as many as count. Default is 5.
Datagram size [100]	Ping packet size. Default is 100 bytes.
Timeout in seconds [2]	It is considered as successful ping test if reply returns within the configured time interval. Default is 2 seconds.
Extended commands [n]	Shows the additional commands. Default is no.

Tab. 6.2 Options for Ping

The following is an example of ping test 5 times to verify network status with IP address 172.16.1.254.

```
SWITCH# ping
Protocol [ip]: ip
Target IP address: 172.16.1.254
Repeat count [5]: 5
Datagram size [100]: 100
Timeout in seconds [2]: 2
Extended commands [n]: n
PING 172.16.1.254 (172.16.1.254) 100(128) bytes of data.
Warning: time of day goes back (-394us), taking countermeasures.
108 bytes from 172.16.1.254: icmp_seq=1 ttl=255 time=0.058 ms
108 bytes from 172.16.1.254: icmp_seq=2 ttl=255 time=0.400 ms
108 bytes from 172.16.1.254: icmp_seq=3 ttl=255 time=0.403 ms
108 bytes from 172.16.1.254: icmp_seq=4 ttl=255 time=1.63 ms
108 bytes from 172.16.1.254: icmp_seq=5 ttl=255 time=0.414 ms
--- 172.16.1.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 8008ms
rtt min/avg/max/mdev = 0.058/0.581/1.632/0.542 ms
SWITCH#
```

When multiple IP addresses are assigned to the switch, sometimes you need to verify the connection status between the specific IP address and network status.

In this case, use the same process as ping test and then input the followings after extended commands. It is possible to verify the connection between specific IP address and network using the following command.

The following is the information to use ping test for multiple IP addresses.

Items	Description
Source address or interface	Designates the address where the relative device should respond in source ip address.
Type of service [0]:	The service filed of QoS (Quality Of Service) in Layer 3 application. It is possible to designate the priority for IP Packet.
Set DF bit in IP header? [no]	Decides whether Don't Fragment (DB) bit is applied to Ping packet or not. Default is no. If the user choose 'yes', when the packets pass through the segment compromised with the smaller data unit, it prevents the packet to be Fragment. Therefore there could be error message.
Data pattern [0xABCD]	Configures data pattern. Default is 0xABCD.

Tab. 6.3 Options for Ping for Multiple IP Addresses

The following is to verify network status between 172.16.157.100 and 172.16.1.254 when IP address of the switch is configured as 172.16.157.100.

```

SWITCH# ping
Protocol [ip]:
Target IP address: 172.16.1.254
Repeat count [5]: 5
Datagram size [100]: 100
Timeout in seconds [2]: 2
Extended commands [n]: y
Source address or interface: 172.16.157.100
Type of service [0]: 0
Set DF bit in IP header? [no]: no
Data pattern [0xABCD]:
PATTERN: 0xabcd
PING 172.16.1.254 (172.16.1.254) from 172.16.157.100 : 100(128) bytes of data.
108 bytes from 172.16.1.254: icmp_seq=1 ttl=255 time=30.4 ms
108 bytes from 172.16.1.254: icmp_seq=2 ttl=255 time=11.9 ms
108 bytes from 172.16.1.254: icmp_seq=3 ttl=255 time=21.9 ms
108 bytes from 172.16.1.254: icmp_seq=4 ttl=255 time=11.9 ms
108 bytes from 172.16.1.254: icmp_seq=5 ttl=255 time=30.1 ms

--- 172.16.1.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 8050ms
rtt min/avg/max/mdev = 11.972/21.301/30.411/8.200 ms
SWITCH#

```

6.3.2 IP ICMP Source-Routing

If you implement PING test to verify the status of network connection, icmp request arrives at the final destination as the closest route according to the routing theory.

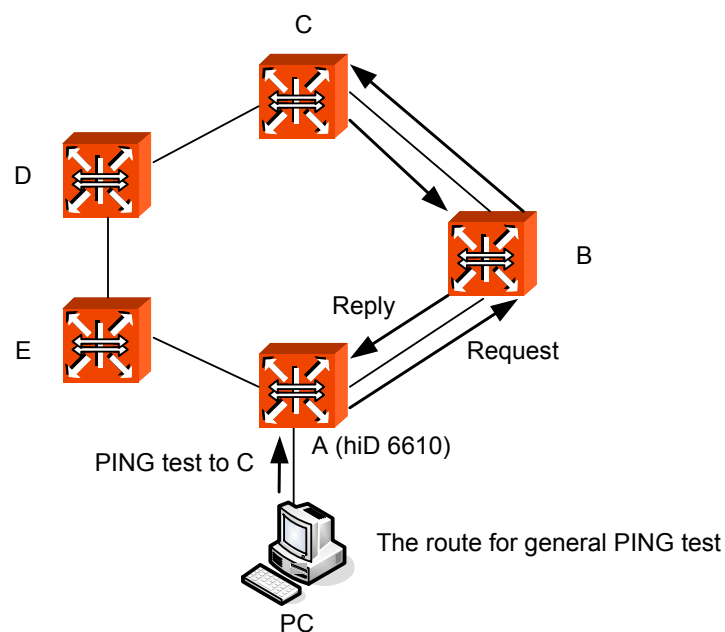


Fig. 6.1 Ping Test for Network Status

In the above figure, if you perform ping test from PC to C, it goes through the route of 「A→B→C」. This is the general case. But, the hiD 6610 S311 can enable to perform ping test from PC as the route of 「A→E→D→C」.

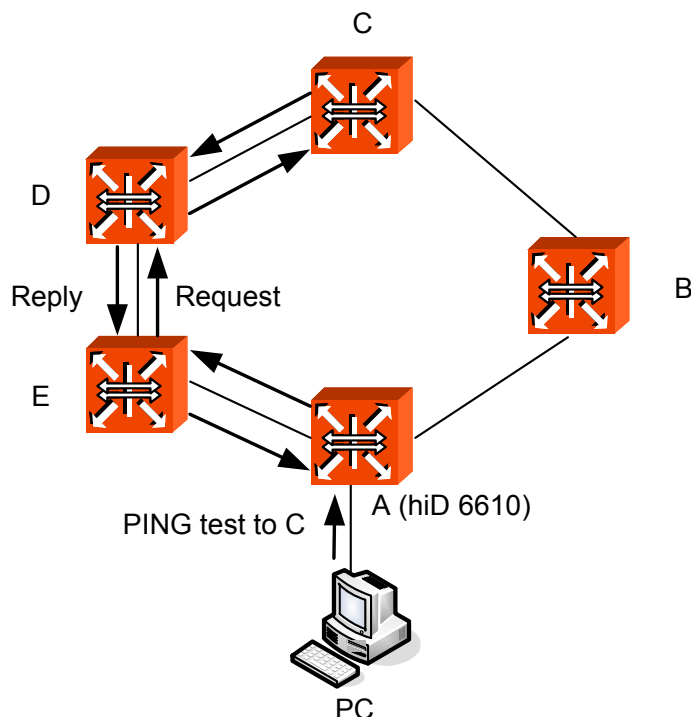


Fig. 6.2 IP Source Routing

To perform ping test as the route which the manager designated, use the following steps.

Step 1

Enable IP source-routing function from the equipment connected to PC which the PING test is going to be performed.

To enable/disable IP source-routing in the hiD 6610 S311, use the following command.

Command	Mode	Description
ip icmp source-route	Global	Enable IP source-routing function.
no ip icmp source-route		Disable IP source-routing function.

Step 2

Performs the ping test from PC as the designate route with the **ping** command

6.3.3 Tracing Packet Route

You can discover the routes that packets will actually take when traveling to their destinations. To do this, the **tracert** command sends probe datagram and displays the round-trip time for each node.

If the timer goes off before a response comes in, an asterisk (*) is printed on the screen.

Command	Mode	Description
tracert [ADDRESS]	Enable	Traces packet routes through the network. ADDRESS: IP address or host name
tracert ip ADDRESS		

The following is the basic information to trace packet routes.

Items	Description
Protocol [ip]	Supports ping test. Default is IP.
Target IP address	Sends ICMP echo message by inputting IP address or host name of destination in order to check network status with relative.
Source address	Source IP address which other side should make a response.
Numeric display [n]	Hop is displayed the number instead of indications or statistics.
Timeout in seconds [2]	It is considered as successful ping test if reply returns within the configured time interval. Default is 2 seconds.
Probe count [3]	Set the frequency of probing UDP packets.
Maximum time to live [30]	The TTL field is reduced by one on every hop. Set the time to trace hop transmission (The number of maximum hops). Default is 30 seconds.
Port Number [33434]	Selects general UDP port to be used for probing Port. The default is 33434. The command of tracert depends on the port range of destination host up to base + nhops – 1 through the base.

Tab. 6.4 Options for Tracing Packet Route

The following is an example of tracing packet route sent to 10.2.2.20.

```
SWITCH# tracert 10.2.2.20
tracert to 10.2.2.20 (10.2.2.20), 30 hops max, 38 byte packets
1 10.2.2.20 (10.2.2.20) 0.598 ms 0.418 ms 0.301 ms
SWITCH#
```

6.3.4 Displaying User Connecting to System

To display current users connecting to the system from a remote place or via console interface, use the following command.

Command	Mode	Description
where	Enable	Shows current users connecting to the system from a remote place or via console interface.

The following is an example of displaying if there is any accessing user from remote place.

```
SWITCH# where
admin at tty0 from 10.20.1.32:2196 for 30 minutes 35.56 seconds
admin at ttyS0 from console for 28 minutes 10.90 seconds
SWITCH#
```

6.3.5 MAC Table

To display MAC table recorded in specific port, use the following command.

Command	Mode	Description
show mac <i>BRIDGE</i> [<i>PORTS</i>]	Enable Global Bridge	Shows MAC table. BRIDGE: bridge name

The following is an example of displaying MAC table recorded in default.

```
SWITCH(config)# show mac 1

port          mac addr          permission    in use
=====
eth01         00:0b:5d:98:92:da   OK            16.62
eth01         00:14:c2:d9:8a:b5   OK            56.62
eth01         00:01:02:50:d6:b9   OK            72.62
eth01         00:0d:9d:8c:00:ee   OK            72.62
eth01         00:15:00:39:4d:2e   OK            92.62
eth01         00:0e:e8:8b:24:ae   OK            115.48
eth01         00:14:c2:d9:4c:f0   OK            115.48
eth01         00:0b:5d:53:4d:96   OK            124.62
eth01         00:13:20:4b:05:af   OK            132.62
eth01         00:0e:e8:f0:b3:63   OK            152.62
(skipped)
SWITCH(config)#
```

6.3.6 Running Time of System

To display running time of the system, use the following command.

Command	Mode	Description
show uptime	Enable Global	Shows running time of the system.

The following is an example of displaying running time of the system.

```
SWITCH# show uptime
10:41am up 15 days, 10:55, 0 users, load average: 0.05, 0.07, 0.01
SWITCH#
```

6.3.7 System Information

To display the system information, use the following command.

Command	Mode	Description
show system	Enable Global	Shows the system information.

The following is an example of displaying the system information of hiD 6610 S311.

```
SWITCH(config)# show system

      SysInfo(System Information)
Model Name       : SURPASS hiD6610 S311
Main Memory Size : 128 MB
Flash Memory Size : 8 MB(INTEL 28F640J3), 32 MB(INTEL 28F256J3)
S/W Compatibility : 3, 7
H/W Revision     : DS-T3-07F-A2
NOS Version      : 3.06
B/L Version      : 4.69
H/W Address      : 00:d0:cb:27:01:66
PLD Version      : 0x10
Serial Number    : N/A
SWITCH(config)#
```

6.3.8 System Memory Information

To display a system memory status, use the following command.

Command	Mode	Description
show memory	Enable Global	Shows system memory information.
show memory {bgp dhcp imi lib nsm ospf pim rip}		Shows system memory information with a specific option.

6.3.9 Average of CPU Load

It is possible to display average of CPU load using the following command.

Command	Mode	Description
show cpuload	View Enable Global	Shows threshold of CPU utilization and average of CPU utilization.

6.3.10 Statistics of CPU Load

It is possible to display CPU load statistics using the following command.

Command	Mode	Description
show cpu statistics avg-pkt <i>PORTS</i>	Enable Global	Shows the CPU statistics of the average of multi-cast/broadcast packets.
show cpu statistics total <i>PORTS</i>		Shows the CPU statistics of all the packets of uni-cast/multicast/broadcast.

The following is an example of displaying the statistics of CPU load.

```
SWITCH# show cpu statistics total 26
=====
Port | Tx | Rx
-----|-----|-----
Time | pkts | bits | pkts | bits
=====
port 26 -----
Ucast:      961      623,816      1,310      672,792
Mcast:        0         0      32,548      16,677,064
Bcast:        0         0      71,313      50,688,176

SWITCH# show cpu statistics avg-pkt 26
=====
Port | Tx | Rx
-----|-----|-----
Time | pkts/s | bits/s | pkts/s | bits/s
=====
port 26 -----
Ucast
  5 sec:      1        512        1        920
  1 min:      3      2,832        3      1,952
 10 min:      0        688        1        520
Mcast
  5 sec:      0         0        0        200
  1 min:      0         0        0        256
 10 min:      0         0        0        256
Bcast
  5 sec:      0         0        2      1,480
  1 min:      0         0        0        544
 10 min:      0         0        1      1,024
SWITCH#
```

6.3.11 Running Process

The hiD 6610 S311 provides a function that shows information of the running processes. The information with this command can be very useful to manage the switch.

To display information of the running processes, use the following command.

Command	Mode	Description
show process	Enable Global	Shows information of the running processes.

The following is an example of displaying information of the running processes.

```
SWITCH# show process
USER      PID  %CPU  %MEM    VSZ   RSS  TTY   STAT   START   TIME  COMMAND
admin      1   0.2   0.2   1448   596  ?     S       20:12  0:05  init [3]
admin      2   0.0   0.0     0     0  ?     S       20:12  0:00  [keventd]
admin      3   0.0   0.0     0     0  ?     SN      20:12  0:00  [ksoftirqd_CPU0]
admin      4   0.0   0.0     0     0  ?     S       20:12  0:00  [kswapd]
admin      5   0.0   0.0     0     0  ?     S       20:12  0:00  [bdf flush]
admin      6   0.0   0.0     0     0  ?     S       20:12  0:00  [kupdated]
admin      7   0.0   0.0     0     0  ?     S       20:12  0:00  [mtdblockd]
admin      8   0.0   0.0     0     0  ?     SW<     20:12  0:00  [bcmDPC]
admin      9   1.4   0.0     0     0  ?     SW<     20:12  0:29  [bcmCNTR.0]
admin     10   1.4   0.0     0     0  ?     SW<     20:12  0:29  [bcmCNTR.1]
admin     17   0.0   0.0     0     0  ?     SWN      20:12  0:00  [jffs2_gcd_mtd3]
admin    149   0.0   0.3   1784   776  ?     S       Jan01  0:00  /sbin/syslogd -m
admin    151   0.0   0.2   1428   544  ?     S       Jan01  0:00  /sbin/klogd -c 1
admin    103   2.6   2.0  20552  5100  ?     S       20:12  0:53  /usr/sbin/swchd
--more--
(Omitted)
SWITCH#
```

6.3.12 Displaying System Image

To check a current system image version, use the following command.

Command	Mode	Description
show version	Enable Global	Shows version of system image.

To display a size of the current system image, use the following command.

Command	Mode	Description
show os-size	Enable Global	Shows size of system image.

6.3.13 Displaying Installed OS

To display utilization of flash memory, use the following command.

Command	Mode	Description
show flash	Enable Global	Shows utilization of flash memory.

6.3.14 Default OS

The hiD 6610 S311 supports dual OS. You can show the flash memory by using the **show system** command. When there are two kinds of system images installed, user can configure one of two as default OS what user wants.

In hiD 6610 S311, a system image saved in **os1** is configured as default OS by default.

To designate a default OS, use the following command.

Command	Mode	Description
default-os {os1 os2}	Enable	Designates default OS of switch.

6.3.15 Switch Status

To display temperature of switch, power status, and fan status, use the following command.

Command	Mode	Description
show status fan	Enable Global Bridge	Shows fan status of switch.
show status power		Shows power status.
show status temp		Shows temperature of switch.

6.3.16 Tech Support

In hiD 6610 S311, you can display the configuration and configuration file, log information, register, memory, debugging information using the following commands. By checking tech supporting, check the system errors and use it for solving the problem.

Command	Mode	Description
tech-support {all crash-info} console	Enable	Check tech support on console.
tech-support {all crash-info} remote IP-ADDRESS {ftp tftp}		Save the contents of tech support in a specified address.



Tech support contents displayed on console are showed at once regardless of the number of display lines of terminal screen.

7 Network Management

7.1 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) system is consisted of three parts: SNMP manager, a managed device and SNMP agent. SNMP is an application-layer protocol that allows SNMP manager and agent stations to communicate with each other. SNMP provides a message format for sending information between SNMP manager and SNMP agent. The agent and MIB reside on the switch. In configuring SNMP on the switch, you define the relationship between the manager and the agent. According to community, you can give right only to read or right both to read and to write. The SNMP agent has MIB variables to reply to request from SNMP administrator. And SNMP administrator can obtain data from the agent and save data in the agent. The SNMP agent gets data from MIB, which saves information on system and network.

SNMP agent sends trap to administrator for specific cases. Trap is a warning message to alert network status to SNMP administrator.

The hiD 6610 S311 enhances accessing management of SNMP agent more and limit the range of OID opened to agents.

The following is how to configure SNMP.

- SNMP Community
- Information of SNMP Agent
- SNMP Com2sec
- SNMP Group
- SNMP View Record
- Permission to Access SNMP View Record
- SNMP Version 3 User
- SNMP Trap
- SNMP Alarm
- Displaying SNMP Configuration
- Disabling SNMP

7.1.1 SNMP Community

Only an authorized person can access an SNMP agent by configuring SNMP community with a community name and additional information.

To configure an SNMP community to allow an authorized person to access, use the following command on *Global configuration* mode.

Command	Mode	Description
snmp community {ro rw} <i>COMMUNITY</i> [<i>IP-ADDRESS</i>] [<i>OID</i>]	Global	Creates SNMP community. COMMUNITY: community name
no snmp community {ro rw} <i>COMMUNITY</i>		Deletes a created community. COMMUNITY: community name



You can configure up to 3 SNMP communities for each read-only and read-write.

To display a configured SNMP community, use the following command.

Command	Mode	Description
show snmp community	Enable Global	Shows a created SNMP community.

The following is an example of creating 2 SNMP communities.

```
SWITCH(config)# snmp community ro public
SWITCH(config)# snmp community rw private
SWITCH(config)# show snmp community

Community List
Type Community      Source      OID
-----
ro    public
rw    private

SWITCH(config)#
```

7.1.2 Information of SNMP Agent

You can specify basic information of SNMP agent as administrator, location, and address that confirm its own identity.

To set basic information of SNMP agent, use the following command.

Command	Mode	Description
snmp contact <i>NAME</i>	Global	Sets a name of administrator.
snmp location <i>LOCATION</i>		Sets a location of SNMP agent.
snmp agent-address <i>IP-ADDRESS</i>		Sets an IP address of SNMP agent.
no snmp contact		Deletes specified basic information for each item.
no snmp location		
no snmp agent-address <i>IP-ADDRESS</i>		

The following is an example of specifying basic information of SNMP agent.

```
SWITCH(config)# snmp contact Brad
SWITCH(config)# snmp location Germany
SWITCH(config)#
```

To display basic information of SNMP agent, use the following command.

Command	Mode	Description
show snmp contact	Enable Global	Shows a name of administrator.
show snmp location		Shows a location of SNMP agent.
show snmp agent-address		Shows an IP address of SNMP agent.

7.1.3 SNMP Com2sec

SNMP v2 authorizes the host to access the agent according to the identity of the host and community name. The command, **com2sec**, specifies the mapping from the identity of the host and community name to security name.

To configure an SNMP security name, use the following command.

Command	Mode	Description
snmp com2sec <i>SECURITY</i> { <i>IP-ADDRESS</i> <i>IP-ADDRESS/M</i> } <i>COMMUNITY</i>	Global	Specifies the mapping from the identity of the host and community name to security name, enter security and community name. SECURITY: security name COMMUNITY: community name
no snmp com2sec <i>SECURITY</i>		Deletes a specified security name, enter the security name. SECURITY: security name
show snmp com2sec	Enable Global	Shows a specified security name.

The following is an example of configuring SNMP com2sec.

```
SWITCH(config)# snmp com2sec TEST 10.1.1.1 PUBLIC
SWITCH(config)# show snmp com2sec

Com2Sec List
      SecName  Source  Community
-----
com2sec  TEST      10.1.1.1 PUBLIC

SWITCH(config)#
```

7.1.4 SNMP Group

You can create an SNMP group that can access SNMP agent and its community that belongs to a group.

To create an SNMP group, use the following command.

Command	Mode	Description
snmp group <i>GROUP</i> { <i>v1</i> <i>v2c</i> <i>v3</i> } <i>SECURITY</i>	Global	Creates SNMP group, enter the group name. GROUP: group name SECURITY: security name
no snmp group <i>GROUP</i> { <i>v1</i> <i>v2c</i> <i>v3</i> } <i>SECURITY</i>		Deletes SNMP group, enter the group name. GROUP: group name
show snmp group	Enable Global	Shows a created SNMP group.

7.1.5 SNMP View Record

You can create an SNMP view record to limit access to MIB objects with object identity (OID) by an SNMP manager.

To configure an SNMP view record, use the following command.

Command	Mode	Description
snmp view <i>VIEW</i> { included excluded } <i>OID</i> [<i>MASK</i>]	Global	Creates an SNMP view record. VIEW: view record name included: includes sub-tree. excluded: excludes sub-tree. OID: OID number MASK: Mask value (e.g. ff ff.ff)
no snmp view <i>VIEW</i> [<i>OID</i>]		Deletes a created SNMP view record. VIEW: view record name

To display a created SNMP view record, use the following command.

Command	Mode	Description
show snmp view	Enable Global	Shows a created SNMP view record.

The following is an example of creating an SNMP view record.

```
SWITCH(config)# snmp view TEST included 410
SWITCH(config)# show snmp view

View list
-----
view TEST included 410

SWITCH(config)#
```

7.1.6 Permission to Access SNMP View Record

To grant an SNMP group to access a specific SNMP view record, use the following command.

Command	Mode	Description
snmp access <i>GROUP</i> { v1 v2c } <i>READ-VIEW WRITE-VIEW NO-</i> <i>TIFY-VIEW</i>	Global	Grants an SNMP group to access a specific SNMP view record. GROUP: group name
snmp access <i>GROUP</i> v3 { no-auth auth priv } <i>READ-VIEW</i> <i>WRITE-VIEW NOTIFY-VIEW</i>		Grants an SNMP version 3 group to access a specific SNMP view record. GROUP: group name
no snmp access <i>GROUP</i>		Deletes a granted SNMP group to access a specific SNMP view record.

To display a granted an SNMP group to access a specific SNMP view record, use the following command.

Command	Mode	Description
show snmp access	Enable Global	Shows a granted an SNMP group to access a specific SNMP view record

The following is an example of permission to accessing an SNMP view record.

```
SWITCH(config)#
SWITCH(config)# snmp access regroup v1 test none none
SWITCH(config)# show snmp access
Access List
GroupName      SecModel SecLevel ReadView      WriteView      NotifyView
-----
rogroup        v1        noauth  TEST        none          none
SWITCH(config)#
```

7.1.7 SNMP Version 3 User

In SNMP version 3, you can register an SNMP agent as user. If you register SNMP version 3 user, you should configure it with the authentication key.

To create/delete SNMP version 3 user, use the following command.

Command	Mode	Description
snmp user USER {md5 sha} AUTH-KEY[des PRIVATE-KEY]	Global	Creates SNMP version 3 user. USER : enters user name AUTH-KEY: Authentication passphrase (min length:8) PRIVATE-KEY: Privacy passphrase (min length: 8)
no snmp user USER		Deletes a registered SNMP version 3 user.

To display SNMP version 3 user, use the following command.

Command	Mode	Description
show snmp user	Enable Global	Displays SNMP version 3 user.

7.1.8 SNMP Trap

SNMP trap is an alert message that SNMP agent notifies SNMP manager about certain problems. If you configure SNMP trap, switch transmits pertinent information to network management program. In this case, trap message receivers are called trap host.

7.1.8.1 SNMP Trap Host

To set an SNMP trap host, use the following command.

Command	Mode	Description
snmp trap-host <i>IP-ADDRESS [COMMUNITY]</i>	Global	Specifies IP address of an SNMP trap host.
snmp trap2-host <i>IP-ADDRESS [COMMUNITY]</i>		
snmp inform-trap-host <i>IP-ADDRESS [COMMUNITY]</i>		Specifies IP address of SNMP information trap host.



You need to configure an SNMP trap host with the **snmp trap2-host** command, if you manage the switch via the ACI-E.

To delete a specified SNMP trap host, use the following command.

Command	Mode	Description
no snmp trap-host <i>IP-ADDRESS</i>	Global	Deletes a specified SNMP trap host.
no snmp trap2-host <i>IP-ADDRESS</i>		
no snmp inform-trap-host <i>IP-ADDRESS</i>		Deletes a specified information trap host.



You can set maximum 16 SNMP trap hosts with inputting one by one.

The following is an example of setting an SNMP trap host.

```
SWITCH(config)# snmp trap-host 10.1.1.3
SWITCH(config)# snmp trap-host 20.1.1.5
SWITCH(config)# snmp trap-host 30.1.1.2
SWITCH(config)#
```

7.1.8.2 SNMP Trap Mode

To select an SNMP trap-mode, use the following command.

Command	Mode	Description
snmp trap-mode {alarm-report event}	Global	Selects SNMP trap-mode according to user's network environment. (alarm-report or event)

- “**event**” **trap-mode** is set by default. It means that Dasan trap OID will be used upon sending the trap if the trap-mode is “event”
- “**alarm-report**” **trap-mode** will be used form SLE MIB OID which is Siemens private OID.



In order to manage hiD 6610 S311 using ACI-E, the trap-mode must be set as “alarm-report”. Otherwise, ACI-E would not recognize any traps set from the hiD 6610 S311.

7.1.8.3 Enabling SNMP Trap

The system provides various kind of SNMP trap, but it may inefficiently work if all these trap messages are sent very frequently. Therefore, you can select each SNMP trap sent to an SNMP trap host.



The system is configured to send all the SNMP traps as default.

- **authentication-failure** is shown to inform wrong community is input when user trying to access to SNMP inputs wrong community.
- **cold-start** is shown when SNMP agent is turned off and restarts again.
- **link-up/down** is shown when network of port specified by user is disconnected, or when the network is connected again.
- **memory-threshold** is shown when memory usage exceeds the threshold specified by user. Also, when memory usage falls below the threshold, trap message will be shown to notify it.
- **cpu-threshold** is shown when CPU utilization exceeds the threshold specified by user. Also, when CPU load falls below the threshold, trap message will be shown to notify it.
- **port-threshold** is shown when the port traffic exceeds the threshold configured by user. Also, when port traffic falls below the threshold, trap message will be shown.
- **temperature-threshold** is shown when the system temperature exceeds the threshold configured by user. Also, when system temperature falls below the threshold, trap message will be shown.
- **dhcp-lease** is shown when there is no more IP address can be assigned in subnet of DHCP server. Even if only one subnet does not have IP address to assign when there are several subnets, this trap message will be seen.
- **fan/power/module** is shown when there is any status-change of fan, power, and module.

To enable SNMP trap, use the following command.

Command	Mode	Description
snmp trap auth-fail	Global	Configures the system to send SNMP trap when SNMP authentication is fail.
snmp trap cold-start		Configures the system to send SNMP trap when SNMP agent restarts.
snmp trap link-up PORTS [NODE]		Configures the system to send SNMP trap when a port is connected to network.
snmp trap link-down PORTS [NODE]		Configures the system to send SNMP trap when a port is disconnected from network.
snmp trap cpu-threshold		Configures the system to send SNMP trap when CPU load exceeds or falls below the threshold.
snmp trap port-threshold		Configures the system to send SNMP trap when the port traffic exceeds or falls below the threshold.
snmp trap temp-threshold		Configures the system to send SNMP trap when system temperature exceeds or falls below the threshold.

Command	Mode	Description
snmp trap dhcp-lease	Global	Configures the system to send SNMP trap when no more IP address that can be assigned in the subnet of DHCP server is left.
snmp trap fan		Configures the system to send SNMP trap when the fan begins to operate or stops.
snmp trap power		Configures the system to send SNMP trap when any problem occurs in power.
snmp trap module		Configures the system to send SNMP trap when there is any problem in module.

7.1.8.4 Disabling SNMP Trap

To disable SNMP trap, use the following command.

Command	Mode	Description
no snmp trap auth-fail	Global	Disables each SNMP trap.
no snmp trap cold-start		
no snmp trap link-up <i>PORTS</i> [<i>NODE</i>]		
no snmp trap link-down <i>PORTS</i> [<i>NODE</i>]		
no snmp trap cpu-threshold		
no snmp trap port-threshold		
no snmp trap temp-threshold		
no snmp trap dhcp-lease		
no snmp trap fan		
no snmp trap power		
no snmp trap module		



When you use the **no snmp** command, all configurations concerning SNMP will be deleted.

7.1.8.5 Displaying SNMP Trap

To display a configuration of SNMP trap, use the following command.

Command	Mode	Description
show snmp trap	Enable Global	Shows a configuration of SNMP trap.

The following is an example of configuring IP address 10.1.1.1 as trap-host, 20.1.1.1 as trap2-host and 30.1.1.1 as inform-trap-host.

```

SWITCH(config)# snmp trap-host 10.1.1.1
SWITCH(config)# snmp trap2-host 20.1.1.1
SWITCH(config)# snmp inform-trap-host 30.1.1.1
SWITCH(config)# show snmp trap

```

Trap-Host List

	Host	Community
inform-trap-host	30.1.1.1	
trap2-host	20.1.1.1	
trap-host	10.1.1.1	

Trap List

Trap-type	Status
auth-fail	enable
cold-start	enable
cpu-threshold	enable
port-threshold	enable
dhcp-lease	enable
power	enable
module	enable
fan	enable
temp-threshold	enable

```

SWITCH(config)#

```

7.1.9 SNMP Alarm

The hiD 6610 S311 provides an alarm notification function. The alarm will be sent to a SNMP trap host whenever a specific event in the system occurs through CLI and ACI-E. You can also set the alarm severity on each alarm and make the alarm be shown only in case of selected severity or higher. This enhanced alarm notification allows system administrators to manage the system efficiently.

7.1.9.1 Enabling Alarm Notification

To configure whether the switch enable transmitting SNMP alarm or not, use the following command.

Command	Mode	Description
snmp notify-activity {enable disable}	Global	Enables/disables an alarm notification on CLI or ACI-E. (default: disable)

7.1.9.2 Default Alarm Severity

To configure a priority of alarm, use the following command.

Command	Mode	Description
snmp alarm-severity default {critical major minor warning intermediate}	Global	Configures the priority of alarm. (default: minor)

7.1.9.3 Alarm Severity Criterion

You can set an alarm severity criterion to make an alarm be shown only in case of selected severity or higher. For example, if an alarm severity criterion has been set to **major**, you will see only an alarm whose severity is **major** or **critical**.

To configure alarm-severity criteria in CLI, use the following command.

Command	Mode	Description
snmp alarm-severity criteria {critical major minor warning intermediate}	Global	Configures the severity criterion. (default: warning)



The order of alarm severity is **critical** > **major** > **minor** > **warning** > **intermediate**.



The alarm severity option is valid only in ACI-E.

7.1.9.4 Generic Alarm Severity

To configure generic alarm severity, use the following command.

Command	Mode	Description
snmp alarm-severity fan-fail {critical major minor warning intermediate}	Global	Configures the priority of fan-fail alarm
snmp alarm-severity cold-start {critical major minor warning intermediate}		Configures the priority of cold-start alarm
snmp alarm-severity broadcast-over {critical major minor warning intermediate}		Configures the priority of broadcast-over alarm
snmp alarm-severity cpu-load-over {critical major minor warning intermediate}		Configures the priority of cpu-load-over alarm
snmp alarm-severity dhcp-lease {critical major minor warning intermediate}		Configures the priority of DHCP-lease alarm
snmp alarm-severity dhcp-illegal {critical major minor warning intermediate}		Configures the priority of DHCP-illegal alarm
snmp alarm-severity fan-remove {critical major minor warning intermediate}		Configures the priority of fan-remove alarm
snmp alarm-severity ipconflict {critical major minor warning intermediate}		Configures the priority of IP conflict alarm
snmp alarm-severity memory-over {critical major minor warning intermediate}		Configures the priority of memory-over alarm
snmp alarm-severity mfgd-block {critical major minor warning intermediate}		Configures the priority of MFGD-block alarm
snmp alarm-severity port-link-down {critical major minor warning intermediate}		Configures the priority of port-link-down alarm
snmp alarm-severity port-remove {critical major minor warning intermediate}		Configures the priority of port-remove alarm
snmp alarm-severity port-thread-over {critical major minor warning intermediate}		Configures the priority of port-thread-over alarm.
snmp alarm-severity power-fail {critical major minor warning intermediate}		Configures the priority of power-fail alarm
snmp alarm-severity power-remove {critical major minor warning intermediate}		Configures the priority of power-remove alarm
snmp alarm-severity rmon-alarm-rising {critical major minor warning intermediate}		Configures the priority of RMON-alarm-rising alarm.
snmp alarm-severity rmon-alarm-falling {critical major minor warning intermediate}		Configures the priority of RMON-alarm-falling alarm.
snmp alarm-severity system-restart {critical major minor warning intermediate}		Configures the priority of system-restart alarm.
snmp alarm-severity module-remove {critical major minor warning intermediate}		Configures the priority of module-remove alarm.
snmp alarm-severity temperature-high {critical major minor warning intermediate}		Configures the priority of temperature-high alarm.

If you want to delete a configured alarm severity, use the following command.

Command	Mode	Description
no snmp alarm-severity fan-fail	Global	Deletes a configured alarm severity.
no snmp alarm-severity cold-start		
no snmp alarm-severity broadcast-over		
no snmp alarm-severity cpu-load-over		
no snmp alarm-severity dhcp-lease		
no snmp alarm-severity dhcp-illegal		
no snmp alarm-severity fan-remove		
no snmp alarm-severity ipconflict		
no snmp alarm-severity memory-over		
no snmp alarm-severity mfgd-block		
no snmp alarm-severity port-link-down		
no snmp alarm-severity port-remove		
no snmp alarm-severity port-thread-over		
no snmp alarm-severity power-fail		
no snmp alarm-severity power-remove		
no snmp alarm-severity rmon-alarm-rising		
no snmp alarm-severity rmon-alarm-falling		
no snmp alarm-severity system-restart		
no snmp alarm-severity module-remove		
no snmp alarm-severity temperature-high		

7.1.9.5 ADVA Alarm Severity

To configure a severity of alarms for ADVA status, use the following command.

Command	Mode	Description
snmp alarm-severity adva-fan-fail {critical major minor warning intermediate}	Global	Sends alarm notification with the severity when ADVA informs fan-fail.
snmp alarm-severity adva-if-misconfig {critical major minor warning intermediate}		Sends alarm notification with the severity when ADVA informs there's any mis-configuration.
snmp alarm-severity adva-if-opt-thres {critical major minor warning intermediate}		Sends alarm notification with the severity when ADVA informs traffic is over threshold on optical interface.
snmp alarm-severity adva-if-rcv-fail {critical major minor warning intermediate}		Sends alarm notification with the severity when ADVA informs to fail to receive the packets.
snmp alarm-severity adva-if-sfp-mismatch {critical major minor warning intermediate}		Sends alarm notification with the severity when ADVA informs SFP module is mismatched.

Command	Mode	Description
snmp alarm-severity adva-if-trans-fault {critical major minor warning intermediate}		Sends alarm notification with the severity when ADVA informs to fail to transmit the packets.
snmp alarm-severity adva-psu-fail {critical major minor warning intermediate}		Sends alarm notification with the severity when ADVA informs there's any problem on the power.
snmp alarm-severity adva-temperature {critical major minor warning intermediate}		Sends alarm notification with the severity when ADVA informs there is any problem in temperature.
snmp alarm-severity adva-voltage-high {critical major minor warning intermediate}		Sends alarm notification with the severity when ADVA informs the voltage is high.
snmp alarm-severity adva-voltage-low {critical major minor warning intermediate}		Sends alarm notification with the severity when ADVA informs the voltage is low.

If you want to clear a configured ADVA alarm priority, use the following command.

Command	Mode	Description
no snmp alarm-severity adva-fan-fail	Global	Clears a configured ADVA alarm priority.
no snmp alarm-severity adva-if-misconfig		
no snmp alarm-severity adva-if-opt-thres		
no snmp alarm-severity adva-if-rcv-fail		
no snmp alarm-severity adva-if-sfp-mismatch		
no snmp alarm-severity adva-if-trans-fault		
no snmp alarm-severity adva-psu-fail		
no snmp alarm-severity adva-temperature		
no snmp alarm-severity adva-voltage-high		
no snmp alarm-severity adva-voltage-low		

7.1.9.6 ERP Alarm Severity

To configure a severity of alarms for ERP status, use the following command.

Command	Mode	Description
snmp alarm-severity erp-domain-lotp {critical major minor warning intermediate}	Global	Sends alarm notification with the severity when no test packet has been received within 3 test packet intervals in ERP mechanism.
snmp alarm-severity erp-domain-multi-rm {critical major minor warning intermediate}		Sends alarm notification with the severity when a Multiple RM node is created.

Command	Mode	Description
snmp alarm-severity erp-domain-reach-fail {critical major minor warning intermediate}	Global	Sends alarm notification with the severity when there is disconnection between ERP domains
snmp alarm-severity erp-domain-ulotp {critical major minor warning intermediate}		Sends alarm notification with the severity when no test packet has been received within 3 test packet intervals in one ERP port while test packets are received in the other port with ERP state.

To delete a configured severity of alarm for ERP status, use the following command.

Command	Mode	Description
no snmp alarm-severity erp-domain-lotp	Global	Deletes a configured severity of alarm for ERP status.
no snmp alarm-severity erp-domain-multi-rm		
no snmp alarm-severity erp-domain-reach-fail		
no snmp alarm-severity erp-domain-ulotp		

7.1.9.7 STP Guard Alarm Severity

To configure a severity of alarm for STP guard status, use the following command.

Command	Mode	Description
snmp alarm-severity stp-bpdu-guard {critical major minor warning intermediate}	Global	Sends alarm notification with the severity when there is stp-bpdu-guard problem
snmp alarm-severity stp-root-guard {critical major minor warning intermediate}		Sends alarm notification with the severity when there is stp-root-guard problem

To delete a configured severity of alarm for STP guard status, use the following command.

Command	Mode	Description
no snmp alarm-severity stp-bpdu-guard	Global	Deletes a configured severity of alarm for STP guard status.
no snmp alarm-severity stp-root-guard		

7.1.10 Displaying SNMP Configuration

To display all configurations of SNMP, use the following command.

Command	Mode	Description
show snmp	Enable Global	Shows all configurations of SNMP.

To display a configured severity of alarm, use the following commands.

Command	Mode	Description
show snmp alarm-severity	Enable Global	Shows a configured severity of alarm.

To delete a recorded alarm in the system, use the following command.

Command	Mode	Description
snmp clear alarm-history	Enable Global	Deletes a recorded alarm in the system.

The following is an example of showing the transmitted alarm and delete the records.

```
SWITCH(config)# show snmp alarm-history  
cold-start      minor      Fri Mar 25 15:30:56 2005 System booted.  
SWITCH(config)# snmp clear alarm-history  
SWITCH(config)# show snmp alarm-history  
SWITCH(config)#
```

To display a current alarm report, use the following command.

Command	Mode	Description
show snmp alarm-report	Enable Global	Shows a current alarm report.

7.1.11 Disabling SNMP

To disable SNMP feature, use the following command.

Command	Mode	Description
no snmp	Global	Disables SNMP feature.



When you use the above command, all configurations concerning SNMP will be deleted.

7.2 Operation, Administration and Maintenance (OAM)

In the enterprise, Ethernet links and networks have been managed via Simple Network Management Protocol (SNMP). Although SNMP provides a very flexible management solution, it is not always efficient and is sometimes inadequate to the task.

First, using SNMP assumes that the underlying network is operational because SNMP relies on IP connectivity; however, you need management functionality even more when the underlying network is non-operational. Second, SNMP assumes every device is IP accessible. This requires provisioning IP on every device and instituting an IP overlay network even if the ultimate end-user service is an Ethernet service. This is impractical in a carrier environment.

For these reasons, carriers look for management capabilities at every layer of the network. The Ethernet layer has not traditionally offered inherent management capabilities, so the IEEE 802.3ah Ethernet in the First Mile (EFM) task force added the Operations, Administration and Maintenance (OAM) capabilities to Ethernet like interfaces. These management capabilities were introduced to provide some basic OAM function on Ethernet media.

EFM OAM is complementary, not competitive, with SNMP management in that it provides some basic management functions at Layer 2, rather than using Layer 3 and above as required by SNMP over an IP infrastructure. OAM provides single-hop functionality in that it works only between two directly connected Ethernet stations. SNMP can be used to manage the OAM interactions of one Ethernet station with another.

7.2.1 OAM Loopback

For OAM loopback function, both the switch and the host should support OAM function. OAM loopback function enables Loopback function from the user's device to the host, which connected to the user's device and operates it.

To enable/disable local OAM function, use the following command.

Command	Mode	Description
oam local admin enable <i>PORTS</i>	Bridge	Enables local OAM.
oam local admin disable <i>PORTS</i>		Disables local OAM.

To configure loopback function of the host connected to the switch, use the following command.

Command	Mode	Description
oam remote loopback enable <i>PORTS</i>	Bridge	Enables loopback function of peer device.
oam remote loopback disable <i>PORTS</i>		Disables loopback function of peer device.
oam remote loopback start <i>PORTS</i>		Operates loopback.

7.2.2 Local OAM Mode

To configure Local OAM, use the following command.

Command	Mode	Description
oam local mode {active passive} PORTS	Bridge	Configures the mode of local OAM.



Both request and loopback are possible for local OAM active. However, request or loopback is impossible for local OAM passive.

7.2.3 OAM Unidirection

When RX is impossible in local OAM, it is possible to send the information by using TX. To enable/disable the function, use the following command.

Command	Mode	Description
oam local unidirection enable PORTS	Bridge	Sends the information by using TX.
oam local unidirection disable PORTS		Disables to transmit the information by using TX.

7.2.4 Remote OAM

To enable/disable remote OAM, use the following command.

Command	Mode	Description
oam remote oam admin <1-2> enable PORTS	Bridge	Enables remote OAM.
oam remote oam admin <1-2> disable PORTS		Disables remote OAM.

To configure the mode of remote OAM, use the following command.

Command	Mode	Description
oam remote oam mode <1-2> {active passive} PORTS	Bridge	Configures the mode of remote OAM.

To display the information of peer host using OAM function, use the following command.

Command	Mode	Description
oam remote alarm optical <1-3> <0-65535> <i>PORTS</i>	Bridge	Shows the information of peer host using OAM function.
oam remote alarm temperature <0-255> <i>PORTS</i>		
oam remote alarm voltage {min max} <0-65535> <i>PORTS</i>		
oam remote electrical mode {full half} <i>PORTS</i>		
oam remote general autonego <1-4> {enable disable} <i>PORTS</i>		
oam remote general forwarding <3-4> {enable disable} <i>PORTS</i>		
oam remote general speed <1-4> <0-4294967295> <i>PORTS</i>		
oam remote general user <1-4> <i>STRING PORTS</i>		
oam remote system interface {unforced forceA forceB} <i>PORTS</i>		
oam remote system interval <0-255> <i>PORTS</i>		
oam remote system mode {master slave} <i>PORTS</i>		
oam remote system reset <i>PORTS</i>		

7.2.5 Displaying OAM Configuration

To display OAM configuration, use the following command.

Command	Mode	Description
show oam	Enable Global Bridge	Shows OAM configuration.
show oam local [<i>PORTS</i>]		Shows local OAM configuration.
show oam remote [<i>PORTS</i>]		Shows remote OAM configuration.
show oam remote variable <0-255> <0-255> <i>PORTS</i>		Shows remote OAM variable.
show oam remote variable specific <0-255> <0-255> <0-4> <i>PORTS</i>		Shows remote OAM specific variable.

The following is to configure to enable OAM loopback function through 25 port of the switch and operate once.

```
SWITCH(bridge)# oam local admin enable 25
SWITCH(bridge)# oam remote loopback enable 25
SWITCH(bridge)# show oam local 25
LOCAL PORT[25]
```

item	value
admin	ENABLE
mode	ACTIVE
mux action	FORWARD
par action	DISCARD
variable	UNSUPPORT
link event	UNSUPPORT
loopback	SUPPORT(disable)
uni-direction	UNSUPPORT(disable)

```
SWITCH(bridge)# show oam remote 25
REMOTE PORT[25]
```

item	value
mode	ACTIVE
MAC address	00:d0:cb:27:00:94
variable	UNSUPPORT
link event	UNSUPPORT
loopback	SUPPORT(enable)
uni-direction	UNSUPPORT

```
SWITCH(bridge)# oam remote loopback start 25
PORT[25]: The remote DTE loopback is success.
SWITCH(bridge)#
```

7.3 Link Layer Discovery Protocol (LLDP)

Link Layer Discovery Protocol (LLDP) is the function of transmitting data for network management for the switches connected in LAN according to IEEE 802.1ab standard.

7.3.1 LLDP Operation

The hiD 6610 S311 supporting LLDP transmits the management information between near switches. The information carries the management information that can recognize the switches and the function. This information is saved in internal MIB (Management Information Base)

When LLDP starts to operate, the switches send their information to near switches. If there is some change in local status, it sends their changed information to near switch to inform their status. For example, if the port status is disabled, it informs that the port is disabled to near switches. And the switch that receives the information from near switches processes LLDP frame and saves the information of the other switches. The information received from other switches is aged.

7.3.2 Enabling LLDP

To enable LLDP, use the following command.

Command	Mode	Description
lldp enable <i>PORTS</i> [<i>mgmtaddr</i> <i>A.B.C.D</i>]	Bridge	Enables LLDP function on a port. A.B.C.D: IP address that is given to LLDP packet
lldp disable <i>PORTS</i> [<i>mgmtaddr</i> <i>A.B.C.D</i>]		Disables LLDP function.

7.3.3 LLDP Operation Type

If you activated LLDP on a port, configure LLDP operation type.

Each LLDP operation type works as the follow:

- **both**: sends and receive LLDP frame.
- **tx_only**: only sends LLDP frame.
- **rx_only**: only receives LLDP frame.
- **disable**: does not process any LLDP frame.

To configure how to operate LLDP, use the following command.

Command	Mode	Description
lldp adminstatus <i>PORTS</i> { both tx_only rx_only disable }	Bridge	Configurs LLDP operation type. (default: disable)

7.3.4 Basic TLV

LLDP is transmitted through TLV. There are mandatory TLV and optional TLV. In optional TLV, there are basic TLV and organizationally specific TLV. Basic TLV must be in the switch where LLDP is realized, specific TLV can be added according to the feature of the switch.

In hiD 6610 S311, the administrator can enable and disable basic TLV by selecting it. To enable basic TLV by selecting it, use the following command.

Command	Mode	Description
lldp enable <i>PORTS</i> { <i>portdescription</i> <i>sysname</i> <i>sysdescription</i> <i>syscap</i> }	Bridge	Selects basic TLV that is sent in the port. portdescription: Port's description syscap: System's capability sysname: System's name sysdescription: System's description
lldp disable <i>PORTS</i> { <i>portdescription</i> <i>sysname</i> <i>sysdescription</i> <i>syscap</i> }		Disables basic TLV configured to be sent in the port.

7.3.5 LLDP Message

In hiD 6610 S311, it is possible to configure the interval time and times of sending LLDP message. To configure the interval time and times of LLDP message, use the following command.

Command	Mode	Description
lldp msg txinterval <5-32768>	Bridge	Configures the interval of sending LLDP message. The unit is second.
lldp msg txhold <2-10>		Configures the periodic times of LLDP message.



Default for sending LLDP message is 4 times in every 30 seconds.

7.3.6 Interval and Delay Time

In hiD 6610 S311, the administrator can configure the interval time of enabling LLDP frame after configuring LLDP operation type. To configure the interval time of enabling LLDP frame after configuring LLDP operation type, use the following command.

Command	Mode	Description
lldp reinitdelay <1-10>	Bridge	Configures the interval time of enabling LLDP frame from the time of configuring not to process LLDP frame. (default: 2)

To configure delay time of transmitting LLDP frame, use the following command.

Command	Mode	Description
lldp txdelay <1-8192>	Bridge	Configures delay time of transmitting LLDP frame. (default: 2)

7.3.7 Displaying LLDP Configuration

To display LLDP configuration, use the following command.

Command	Mode	Description
show lldp config <i>PORTS</i>	Enable	Shows LLDP configuration.
show lldp remote <i>PORTS</i>	Global	Show statistics for remote entries.
show lldp statistics <i>PORTS</i>	Bridge	Shows LLDP operation and statistics.

To delete an accumulated statistics on the port, use the following command.

Command	Mode	Description
clear lldp statistics <i>PORTS</i>	Global Bridge	Deletes an accumulated statistics on the port.

The following is to configure to enable LLDP function on *Bridge Configuration* mode-through port number 10 of the switch and operate it.

```

SWITCH(bridge)# show lldp config 10
GLOBL:
-----
MsgTxInterval    = 30
MsgTxHold        = 4    =>  txTTL = 120
ReInitDelay      = 2
TxDelay          = 2
-----
PORTS active    adminStat|optTLVs
  10: disable   Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
SWITCH(bridge)# lldp enable 10
SWITCH(bridge)# lldp disable 10 portdescription
SWITCH(bridge)# lldp adminstatus 10 tx_only
SWITCH(bridge)# lldp msg txinterval 50
SWITCH(bridge)# lldp msg txhold 8
SWITCH(bridge)# show lldp config 10
GLOBL:
-----
MsgTxInterval    = 50
MsgTxHold        = 8    =>  txTTL = 400
ReInitDelay      = 2
TxDelay          = 2
-----
PORTS active    adminStat|optTLVs
  10: enable     Tx only |0xe= SysName, SysDesc, SysCap
SWITCH(bridge)#

```

7.4 Remote Monitoring (RMON)

Remote Monitoring (RMON) is a function to monitor communication status of devices connected to Ethernet at remote place. While SNMP can give information only about the device mounted SNMP agent, RMON gives information about overall segments including devices. Thus, user can manage network more effectively. For instance, in case of SNMP it is possible to be informed traffic about certain ports but through RMON you can monitor traffics occurred in overall network, traffics of each host connected to segment and current status of traffic between hosts.

Since RMON processes quite lots of data, its processor share is very high. Therefore, administrator should take intensive care to prevent performance degradation and not to overload network transmission caused by RMON. There are nine defined RMON MIB groups in RFC 1757: Statistics, History, Alarm, Host, Host Top N, Matrix, Filter, Packet Capture and Event. The system supports two MIB groups of them, most basic ones: Statistics (only for uplink ports) and History.

7.4.1 RMON History

RMON history is periodical sample inquiry of statistical data about each traffic occurred in Ethernet port. Statistical data of all ports are pre-configured to be monitored at 30-minute interval, and 50 statistical data stored in one port. It also allows you to configure the time interval to take the sample and the number of samples you want to save.

The following is an example of displaying the default configuration of RMON history.

```
SWITCH(config)# show rmon-history config 5

RMON History configuration:
=====
history index      : 5
data source        : 0/1 (1)
buckets requested  : 50
buckets granted    : 50
interval time (s)  : 1800
owner              : none
status             : under create

SWITCH(config)#
```

To open *RMON-history* mode, use the following command.

Command	Mode	Description
rmon-history <1-65535>	Global	Opens <i>RMON-history Configuration</i> mode. 1-65535: index number

The following is an example of opening *RMON-history Configuration* mode with index number 5.

```
SWITCH(config)# rmon-history 5
SWITCH(config-rmonhistory[5])#
```

Input a question mark <?> at the system prompt on *RMON Configuration* mode if you want to list available commands.

The following is an example of listing available commands on *RMON Configuration* mode.

```
SWITCH(config-rmonhistory[5])# ?
RMON history configuration commands:
  active           Activate the history
  data-source      Set data source port
  do              To run exec commands in config mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  interval        Define the time interval for the history
  owner           Assign the owner who define and is using the history
                  resources
  requested-buckets Define the bucket count for the interval
  show            Show running system information

SWITCH(config-rmonhistory[5])#
```

7.4.1.1 Source Port of Statistical Data

To specify a source port of statistical data, use the following command.

Command	Mode	Description
data-source <i>NAME</i>	RMON	Specifies a data object ID. NAME: enters a data object ID. (ex. ifindex.n1/port1)

7.4.1.2 Subject of RMON History

To identify subject using RMON history, use the following command.

Command	Mode	Description
owner <i>NAME</i>	RMON	Identifies subject using related data, enter the name (max. 32 characters).

7.4.1.3 Number of Sample Data

To configure the number of sample data of RMON history, use the following command.

Command	Mode	Description
requested-buckets <1-65535>	RMON	Defines a bucket count for the interval, enter the number of buckets. 1-65535: bucket number (default: 50)

7.4.1.4 Interval of Sample Inquiry

To configure the interval of sample inquiry in terms of second, use the following command.

Command	Mode	Description
interval <1-3600>	RMON	Defines the time interval for the history (in seconds), enter the value. (default: 1800)



1 sec is the minimum time which can be selected. But the minimum sampling interval currently is 30 sec, i.e., all intervals will be round up to a multiple of 30 seconds.

7.4.1.5 Activating RMON History

To activate RMON history, use the following command.

Command	Mode	Description
active	RMON	Activates RMON history.



Before activating RMON history, check if your configuration is correct. After RMON history is activated, you cannot change its configuration. If you need to change configuration, you need to delete the RMON history and configure it again.

7.4.1.6 Deleting Configuration of RMON History

When you need to change a configuration of RMON history, you should delete an existing RMON history.

To delete RMON history, use the following command.

Command	Mode	Description
no rmon-history <1-65535>	RMON	Deletes RMON history of specified number, enter the value for deleting.

7.4.1.7 Displaying RMON History

To display RMON history, use the following command.

Command	Mode	Description
show running-config rmon-history	All	Shows a configured RMON history.



Always the last values will be displayed but no more than the number of the granted buckets.

The following is an example of displaying RMON history.

```
SWITCH(config-rmonhistory [5])# show running-config rmon-history
!
rmon-history 5
  owner test
  data-source ifindex.hdlc1
  interval 60
  requested-buckets 25
  active
!
SWITCH(config-rmonhistory [5])#
```

7.4.2 RMON Alarm

There are two ways to compare with the threshold: absolute comparison and delta comparison.

- **Absolute Comparison:** Comparing sample data with the threshold at configured interval, if the data is more than the threshold or less than it, alarm is occurred
- **Delta Comparison:** Comparing difference between current data and the latest data with the threshold, if the data is more than the threshold or less than it, alarm is occurred.

You need to open *RMON Alarm Configuration* mode first to configure RMON alarm.

Command	Mode	Description
rmon-alarm <1-65535>	Global	Opens <i>RMON Alarm Configuration</i> mode. 1-65535: index number

The following is an example of listing available commands on *RMON-alarm Configuration* mode.

```
SWITCH(config)# rmon-alarm 1
SWITCH(config-rmonalarm[1])# ?

RMON alarm configuration commands:

active                Activate the event
do                    To run exec commands in config mode
exit                  End current mode and down to previous mode
falling-event         Associate the falling threshold with an existing RMON
                      event
falling-threshold      Define the falling threshold
help                  Description of the interactive help system
owner                 Assign the owner who define and is using the history
resources
rising-event          Associate the rising threshold with an existing RMON
                      event
rising-threshold      Define the rising threshold
sample-interval        Specify the sampling interval for RMON alarm
sample-type            Define the sampling type
sample-variable        Define the MIB Object for sample variable
show                  Show running system information
```

```

startup-type      Define startup alarm type (default : rising)
write             Write running configuration to memory or terminal

SWITCH(config-rmonalarm[1])#

```

7.4.2.1 Subject of RMON Alarm

User needs to configure RMON alarm and identify subject using many kinds of data from alarm. To identify subject of alarm, use the following command.

Command	Mode	Description
owner <i>NAME</i>	RMON	Identifies subject using related data, enter the name (max. 32 characters).

7.4.2.2 Object of Sample Inquiry

To assign object used for sample inquiry, use the following command.

Command	Mode	Description
sample-variable <i>MIB-OBJECT</i>	RMON	Assigns MIB object used for sample inquiry.

7.4.2.3 Absolute Comparison and Delta Comparison

To compare object selected as sample with the threshold, use the following command.

Command	Mode	Description
sample-type absolute	RMON	Compares object with the threshold directly.

To configure delta comparison, use the following command.

Command	Mode	Description
sample-type delta	RMON	Compares difference between current data and the latest data with the threshold.

7.4.2.4 Upper Bound of Threshold

If you need to occur alarm when object used for sample inquiry is more than upper bound of threshold, you have to configure the upper bound of threshold.

To configure upper bound of threshold, use the following command.

Command	Mode	Description
rising-threshold <i>VALUE</i>	RMON	Configures upper bound of threshold. VALUE: 0-2147483647

After configuring upper bound of threshold, configure to generate RMON event when object is more than configured threshold. Use the following command.

Command	Mode	Description
rising-event <1-65535>	RMON	Configures to generate RMON event when object is more than configured threshold. 1-65535: event index

7.4.2.5 Lower Bound of Threshold

If you need to occur alarm when object used for sample inquiry is less than lower bound of threshold, you should configure lower bound of threshold. To configure lower bound of threshold, use the following command.

Command	Mode	Description
falling-threshold <i>NUMBER</i>	RMON	Configures lower bound of threshold.

After configuring lower bound of threshold, configure to generate RMON event when object is less than configured threshold. Use the following command.

Command	Mode	Description
falling-event <1-65535>	RMON	Configures to generate RMON alarm when object is less than configured threshold.

7.4.2.6 Configuring Standard of the First Alarm

It is possible for users to configure the standard the first time alarm is occurred. The user can select the first point when object is more than threshold, or the first point when object is less than threshold, or the first point when object is more than threshold or less than threshold.

To configure the first RMON alarm to occur when object is less than lower bound of threshold first, use the following command.

Command	Mode	Description
startup-type falling	RMON	Configures the first RMON Alarm to occur when object is less than lower bound of threshold first.

To configure the first alarm to occur when object is firstly more than upper bound of threshold, use the following command.

Command	Mode	Description
startup-type rising	RMON	Configures the first Alarm to occur when object is firstly more than upper bound of threshold.

To configure the first alarm to occur when object is firstly more than threshold or less than threshold, use the following command.

Command	Mode	Description
startup-type rising-and-falling	RMON	Configures the first Alarm to occur when object is firstly more than threshold or less than threshold.

7.4.2.7 Interval of Sample Inquiry

The interval of sample inquiry means time interval to compare selected sample data with upper bound of threshold or lower bound of threshold in terms of seconds.

To configure interval of sample inquiry for RMON alarm, use the following command.

Command	Mode	Description
sample-interval <0-65535>	RMON	Configures interval of sample inquiry. (unit: second)

7.4.2.8 Activating RMON Alarm

After finishing all configurations, you need to activate RMON alarm. To activate RMON alarm, use the following command.

Command	Mode	Description
active	RMON	Activates RMON alarm.

7.4.2.9 Deleting Configuration of RMON Alarm

When you need to change a configuration of RMON alarm, you should delete an existing RMON alarm.

To delete RMON alarm, use the following command.

Command	Mode	Description
no rmon-alarm <1-65535>	Global	Deletes RMON history of specified number, enter the value for deleting.

7.4.2.10 Displaying RMON Alarm

To display RMON alarm, use the following command.

Command	Mode	Description
show running-config rmon-alarm	All	Shows a configured RMON alarm.

7.4.3 RMON Event

RMON event identifies all operations such as RMON alarm in the switch. You can configure event or trap message to be sent to SNMP management server when sending RMON alarm.

You need to open *RMON Event Configuration* mode to configure RMON event.

Command	Mode	Description
rmon-event <1-65535>	Global	Opens <i>RMON Event Configuration</i> mode. 1-65535: index number

7.4.3.1 Event Community

When RMON event is happened, you need to input community to transmit SNMP trap message to host. Community means a password to give message transmission right.

To configure community for trap message transmission, use the following command.

Command	Mode	Description
community NAME	RMON	Configures password for trap message transmission right. NAME: community name

7.4.3.2 Event Description

It is possible to describe event briefly when event is happened. However, the description will not be automatically made. Thus administrator should make the description.

To make a description about event, use the following command.

Command	Mode	Description
description DESCRIPTION	RMON	Describes the event.

7.4.3.3 Subject of RMON Event

You need to configure event and identify subject using various data from event. To identify subject of RMON event, use the following command.

Command	Mode	Description
owner NAME	RMON	Identifies subject of event. You can use maximum 126 characters and this subject should be same with the subject of RMON alarm.

7.4.3.4 Event Type

When RMON event happened, you need to configure event type to arrange where to send event.

To configure event type, use the following command.

Command	Mode	Description
type log	RMON	Configures event type as log type. Event of log type is sent to the place where the log file is made.
type trap		Configures event type as trap type. Event of trap type is sent to SNMP administrator and PC.
type log-and-trap		Configures event type as both log type and trap type.
type none		Configures none event type.

7.4.3.5 Activating RMON Event

After finishing all configurations, you should activate RMON event. To activate RMON event, use the following command.

Command	Mode	Description
active	RMON	Activates RMON event.

7.4.3.6 Deleting Configuration of RMON Event

Before changing the configuration of RMON event, you should delete RMON event of the number and configure it again.

To delete RMON event, use the following command.

Command	Mode	Description
no rmon-event <1-65535>	Global	Delete RMON event of specified number.

7.4.3.7 Displaying RMON Event

To display RMON alarm, use the following command.

Command	Mode	Description
show running-config rmon-event	All	Shows a configured RMON event.

7.5 Syslog

The syslog is a function that allows the network element to generate the event notification and forward it to the event message collector like a syslog server. This function is enabled as default, so even though you disable this function manually, the syslog will be enabled again.

This section contains the following contents.

- Syslog Output Level
- Facility Code
- Syslog
- Enabling Syslog
- Displaying Syslog Message
- Displaying Syslog Configuration

7.5.1 Syslog Output Level

Syslog Output Level without a Priority

To set a syslog output level, use the following command.

Command	Mode	Description
syslog output {emerg alert crit err warning notice info debug} console	Global	Generates a syslog message of selected level or higher and forwards it to the console.
syslog output {emerg alert crit err warning notice info debug} local {volatile non-volatile}		Generates a syslog message of selected level or higher in the system memory. volatile: deletes a syslog message after restart. non-volatile: reserves a syslog message.
syslog output {emerg alert crit err warning notice info debug} remote <i>IP-ADDRESS</i>		Generates a syslog message of selected level or higher and forwards it to a remote host.

To disable a specified syslog output, use the following command.

Command	Mode	Description
no syslog output {emerg alert crit err warning notice info debug} console	Global	Deletes a specified syslog output.
no syslog output {emerg alert crit err warning notice info debug} local {volatile non-volatile}		
no syslog output {emerg alert crit err warning notice info debug} remote <i>IP-ADDRESS</i>		

Syslog Output Level with a Priority

To set a user-defined syslog output level with a priority, use the following command.

Command	Mode	Description
<code>syslog output priority {auth authpriv cron daemon kern local1 local2 local3 local4 local5 local6 local7 lpr mail news syslog user uucp} {emerg alert crit err warning notice info} console</code>	Global	Generates a user-defined syslog message with a priority and forwards it to the console.
<code>syslog output priority {auth authpriv cron daemon kern local1 local2 local3 local4 local5 local6 local7 lpr mail news syslog user uucp} {emerg alert crit err warning notice info} local {volatile non-volatile}</code>		Generates a user-defined syslog message with a priority in the system memory. volatile: deletes a syslog message after restart. non-volatile: reserves a syslog message.
<code>syslog output priority {auth authpriv cron daemon kern local1 local2 local3 local4 local5 local6 local7 lpr mail news syslog user uucp} {emerg alert crit err warning notice info} remote IP-ADDRESS</code>		Generates a user-defined syslog message with a priority and forwards it to a remote host.

To disable a user-defined syslog output level, use the following command.

Command	Mode	Description
<code>no syslog output priority {auth authpriv cron daemon kern local1 local2 local3 local4 local5 local6 local7 lpr mail news syslog user uucp} {emerg alert crit err warning notice info} console</code>	Global	Deletes a specified user-defined syslog output level with a priority.
<code>no syslog output priority {auth authpriv cron daemon kern local1 local2 local3 local4 local5 local6 local7 lpr mail news syslog user uucp} {emerg alert crit err warning notice info} local {volatile non-volatile}</code>		
<code>no syslog output priority {auth authpriv cron daemon kern local1 local2 local3 local4 local5 local6 local7 lpr mail news syslog user uucp} {emerg alert crit err warning notice info} remote IP-ADDRESS</code>		



The order of priority is **emergency** > **alert** > **critical** > **error** > **warning** > **notice** > **info** > **debug**. If you set a specific level of syslog output, you will receive only a syslog message for selected level or higher. If you want receive a syslog message for all the levels, you need to set the level to **debug**.

The following is an example of configuring syslog message to send all logs higher than notice to remote host 10.1.1.1 and configuring local1.info to transmit to console.

```
SWITCH(config)# syslog output notice remote 10.1.1.1
SWITCH(config)# syslog output priority local1 info console
SWITCH(config)# show syslog
System logger on running!

info                local volatile
info                local non-volatile
notice              remote 10.1.1.1
local1.info         console
SWITCH(config)#
```

7.5.2 Facility Code

You can set a facility code of the generated syslog message. This code make a syslog message distinguished from others, so network administrator can handle various syslog messages efficiently.

To set a facility code, use the following command.

Command	Mode	Description
syslog local-code <0-7>	Global	Sets a facility code.
no syslog local-code		Deletes a specified facility code.

The following is an example of configuring priority of all syslog messages which is transmitted to remote host 10.1.1.1, as the facility code 0.

```
SWITCH(config)# syslog output err remote 10.1.1.1
SWITCH(config)# syslog local-code 0
SWITCH(config)# show syslog
System logger on running!

info                local volatile
info                local non-volatile
err                 remote 10.1.1.1
local_code          0
SWITCH(config)#
```

7.5.3 Syslog Bind Address

You can specify IP address to attach to the syslog message for its identity. To specify IP address for syslog identity, use the following command.

Command	Mode	Description
syslog bind-address A.B.C.D	Global	Specifies IP address for a syslog message identity.
no syslog bind-address		Deletes a specified binding IP address.

7.5.4 Debug Message for Remote Terminal

To display a syslog debug message to a remote terminal, use the following command.

Command	Mode	Description
terminal monitor	Enable	Enables a terminal monitor function.
no terminal monitor		Disables a terminal monitor function.



Terminal monitor is not possible to be operational in local console.

7.5.5 Enabling Syslog

To enable/disable the syslog manually, use the following command.

Command	Mode	Description
syslog start	Global	Enables the syslog.
no syslog		Disables the syslog.



The syslog is basically enabled in the system, so the command, **syslog start**, is necessary only when the function is manually disabled by user.

7.5.6 Displaying Syslog Message

To display a received syslog message in the system memory, use the following command.

Command	Mode	Description
show syslog local {volatile non-volatile} [NUMBER]	Enable Global	Shows a received syslog message. volatile: removes a syslog message after restart. non-volatile: reserves a syslog message. NUMBER: shows the last N syslog messages.
show syslog local {volatile non-volatile} reverse		Shows the syslog messages from the latest one.
clear syslog local {volatile non-volatile}	Enable Global	Removes a received syslog message.

7.5.7 Displaying Syslog Configuration

To display a configuration of the syslog, use the following command.

Command	Mode	Description
show syslog	Enable Global	Shows a configuration of the syslog.
show syslog {volatile non-volatile} information		

7.6 Rule and QoS

The hiD 6610 S311 provides rule and QoS feature for traffic management. The rule classifies incoming traffic, and then processes the traffic according to user-defined policies. You can use the physical port, 802.1p priority (CoS), VLAN ID, DSCP, and so on to classify incoming packets.

You can configure the policy in order to change some data fields within a packet or to relay packets to a mirror monitor by a “Rule” function. QoS (Quality of Service) is one of useful functions to provide the more convenient service of network traffic for users. It is very serviceable to prevent overloading and delaying or failing of sending traffic by giving priority to traffic.

By the way, you need to be careful for other traffics not to be failed by the traffic configured as priority by user. QoS can give a priority to a specific traffic by basically offering the priority to the traffic or limiting the others. When processing data, data are usually supposed to be processed in time-order like first in, first out.

This way, not processing specific data first, might lose all data in case of overloading traffics. However, in case of overloading traffics QoS can apply processing order to traffic by reorganizing priorities according to its importance. By favor of QoS, you can predict network performance in advance and manage bandwidth more effectively.

7.6.1 How to Operate Rule and QoS

For the hiD 6610 S311, rules operate as follows.

- Rule Creation
To classify the packets according to the specific basis, configure the policies about them first. The basis used to classify the packets is 802.1p priority (CoS), VLAN ID, DSCP and port number. Additionally, a unique name needs to be assigned to each rule.
- Rule Priority
Assigns a priority to a rule (precedence to other rules).
- Packet Classification
Configures the policy to adjust how and what is to be classified within transmitted packets.
- Rule Match
Configures the policy classifying the action(s) to be performed if the configured rule classification fits transmitted packet(s).
 - **mirror** transmits the classified traffic to monitor port.
 - **redirect** transmits the classified traffic to specified port.
 - **permit** allows traffic matching given characteristics.
 - **deny** blocks traffic matching given characteristics.
- Rule Apply
Applies the just configured rule. Configured values will be checked and the rule becomes activated within the system.



An already applied rule can not be modified. It needs to be deleted and then created again with changed values.

- **Scheduling Algorithm**
To handle overloading of traffics, you need to configure differently processing orders of graphic by using scheduling algorithm. The hiD 6610 S311 provides:
 - Strict Priority Queuing (SPQ)
 - Weighted Round Robin (WRR)
 - Weighted Fair Queuing (WFQ).
- **Queue Weight**
Queue weight can be used to additionally adjust the scheduling mode per queue in WRR or WFQ mode.
 - Queue weight controls the scheduling precedence of the internal packet queues. The higher the weight value the higher the scheduling precedence of this queue.

7.6.2 Rule Configuration

7.6.2.1 Rule Creation

For the hiD 6610 S311, you need to open *Rule Configuration* mode first. To open *Rule Configuration* mode, use the following command.

Command	Mode	Description
rule NAME create	Global	Opens <i>Rule Configuration</i> mode, enter rule name.

After opening *Rule Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-rule[name])#.

After opening *Rule Configuration* mode, a rule can be configured by user. The rule priority, rule match, rule action, and action parameter(s) can be configured for each rule.



1. The rule name must be unique. Its size is limited to 63 significant characters.
2. The order in which the following configuration commands will be entered is arbitrary.
3. The configuration of a rule being configured can be changed as often as wanted (inclusive rule type) until the command, **apply**, will be entered.
4. Use the command, **show rule-profile**, to display the configuration entered up to now.



You can not create the rule name which started with alphabet 'a' If you try to enter 'a', the error message will be appeared. .

7.6.2.2 Rule Priority

If rules that are more than two match the same packet then the rule having a higher priority will be processed first.

To set a priority for a rule, use the following command.

Command	Mode	Description
priority {low medium high highest}	Rule	Sets a priority for a rule.

7.6.2.3 Packet Classification

After configuring a packet classification for a rule, then configure how to process the packets. To specify a packet-classifying pattern, use the following command.



When specifying a source and destination IP address as a packet-classifying pattern, the destination IP address must be after the source IP address.

Command	Mode	Description
port { <i>SRC-PORT</i> any } { <i>DST-PORT</i> cpu any }	Rule	Classifies a physical port: SRC-PORT: source port number DST-PORT: destination port number cpu: CPU port any: any physical port (ignore)
vlan { <i>VID</i> any }		Classifies a VLAN: VLAN: 1-4094 any: any VLAN (ignore)
dscp {<0-63> any }		Classifies a DSCP value: 0-63: DSCP value any: any DSCP (ignore)
cos {<0-7> any }		Classifies the IEEE 802.1p priority: 0-7: 802.1p priority value any: any 802.1p priority value (ignore)
tos {<0-255> any }		Classifies all ToS field: 0-255: ToS value any: any ToS value (ignore)
ip-prec {<0-7> any }		Classifies an IP precedence: 0-7: IP precedence value any: any IP precedence value (ignore)
length {<21-65535> any }		Classifies a packet length: 21-65535: IP packet length any: any IP packet length (ignore)
ethtype { <i>TYPE-NUM</i> arp any }		Classifies the Ethernet type: TYPE-NUM: Ethernet type field (hex, e.g. 0800 for IPv4) arp: address resolution protocol any: any Ethernet type (ignore)
mac { <i>SRC-MAC-ADDRESS</i> any } { <i>DST-MAC-ADDRESS</i> any }		Classifies MAC address: SRC-MAC-ADDRESS: source MAC address DST-MAC-ADDRESS: destination MAC address any: any source/destination MAC address (ignore)
ip { <i>A.B.C.D</i> <i>A.B.C.D/M</i> any } { <i>A.B.C.D</i> <i>A.B.C.D/M</i> any } [0-255]		Classifies an IP address: A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-255: IP protocol number

Command	Mode	Description
ip {A.B.C.D A.B.C.D/M any } {A.B.C.D A.B.C.D/M any } icmp	Rule	Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address icmp: ICMP
ip {A.B.C.D A.B.C.D/M any } {A.B.C.D A.B.C.D/M any } icmp {<0-255> any } [<0-255> any]		Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address icmp: ICMP 0-255: ICMP message type number 0-255: ICMP message code number
ip {A.B.C.D A.B.C.D/M any } {A.B.C.D A.B.C.D/M any } { tcp udp }		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP udp: UDP
ip {A.B.C.D A.B.C.D/M any } {A.B.C.D A.B.C.D/M any } { tcp udp } {<0-65535> any } {<0-65535> any }		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP udp: UDP 0-65535: TCP/UDP source/destination port number any: any TCP/UDP source/destination port
ip {A.B.C.D A.B.C.D/M any } {A.B.C.D A.B.C.D/M any } tcp {<0-65535> any } {<0-65535> any } {TCP-FLAG any }		Classifies an IP protocol (TCP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP 0-65535: TCP source/destination port number any: any TCP source/destination port TCP-FLAG: TCP flag (e.g. S(SYN), F(FIN)) any: any TCP flag

To delete a specified packet-classifying pattern, use the following command.

Command	Mode	Description
no vlan	Rule	Deletes a specified packet-classifying pattern for each option.
no cos		
no tos		
no length		
no ethtype		
no mac		
no ip		

7.6.2.4 Rule Action

To specify a rule action (**match**) for the packets matching configured classifying patterns, use the following command.

Command	Mode	Description
match deny	Rule	Denies a packet.
match permit		Permits a packet.
match redirect <i>PORT</i>		Redirects to specified egress port: PORT: uplink port number
match mirror		Sends a copy to mirror monitoring port.
match dscp <0-63>		Changes DSCP field, enter DSCP value.
match cos <0-7>		Changes 802.1p class of service, enter CoS value. 0-7: CoS value
match cos <0-7> overwrite		Overwrites 802.1p CoS field in the packet. 0-7: CoS value
match cos same-as-tos overwrite		Overwrites 802.1p CoS field in the packet same as IP ToS precedence bits.
match ip-prec <0-7>		Changes IP ToS precedence bits in the packet. 0-7: ToS precedence value
match ip-prec same-as-cos		Changes IP ToS precedence bits in the packet, same as 802.1p CoS value.
match bandwidth <i>BANDWIDTH</i>		Determines maximum allowed bandwidth (Mbps).
match vlan <1-4094>		Specifies matched-packet VLAN ID 1-4094: VLAN ID
match copy-to-cpu		Copies to CPU.
match counter		Counts how many times the packets come into configured Rule.
match dmac <i>DST-MAC-ADDRESS</i>		Overwrites a specified destination MAC address.
match egress filter <i>PORT</i>		Deletes a specified egress port.
match egress port <i>PORT</i>		Overwrites a specified egress port

To delete a specified rule action (**match**), use the following command.

Command	Mode	Description
no match deny	Rule	Deletes a specified rule action.
no match permit		
no match redirect		
no match mirror		
no match dscp		
no match cos		
no match ip-prec		
no match bandwidth		
no match vlan		

Command	Mode	Description
no match copy-to-cpu	Rule	Deletes a specified rule action.
no match counter		
no match dmac		
no match egress		

To specify a rule action (**no-match**) for the packets **not** matching configured classifying patterns, use the following command.

Command	Mode	Description
no-match deny	Rule	Denies a packet.
no-match redirect <i>PORT</i>		Redirects to specified egress port: PORT: uplink port number (e.g. 25-28)
no-match mirror		Sends a copy to mirror monitoring port.
no-match dscp <0-63>		Changes DSCP field, enter DSCP value.
no-match cos <0-7>		Changes 802.1p class of service, enter CoS value. 0-7: CoS value
no-match cos <0-7> overwrite		Overwrites 802.1p CoS field in the packet. 0-7: CoS value
no-match cos same-as-tos-overwrite		Overwrites 802.1p CoS field in the packet same as IP ToS precedence bits.
no-match ip-prec <0-7>		Changes IP ToS precedence bits in the packet. 0-7: ToS precedence value
no-match ip-prec same-as-cos		Changes IP ToS precedence bits in the packet, same as 802.1p CoS value.
no-match copy-to-cpu		Copies to CPU.

To delete a specified rule action (**no-match**), use the following command.

Command	Mode	Description
no no-match deny	Rule	Deletes a specified rule action.
no no-match redirect		
no no-match mirror		
no no-match dscp		
no no-match cos		
no no-match ip-prec		
no no-match copy-to-cpu		

7.6.2.5 Applying Rule

After configuring rule using the above commands, apply it to the system with the following command. If you do not apply the rule to the system, all specified rules will be lost.

To save and apply a rule, use the following command.

Command	Mode	Description
apply	Rule	Applies a rule to the system.



1. The switch performs a detailed plausibility check and rejects the rule if the configuration is incomplete, contains bad or unsupported values or conflicts to other rules. In this case, the switch informs about the reason and the operator may correct the values
2. The switch may reject a rule with the message "% Already exist rule" although the name will not be listed by command, **show rule**. Unfortunately, the entered name in this case interferes with the name of an internally managed rule.
Remedy: Select another name for the rule (e.g. add a prefix).
3. All previously entered values remain valid after successful (or unsuccessful) execution of command, **apply**. That is, if several rules being different only in one value should be created, then only the one changed value needs to be entered again.

7.6.2.6 Modifying and Deleting Rule

To modify a rule, use the following command.

Command	Mode	Description
rule NAME modify	Global	Modifies a rule, enter a rule name.

To delete a rule, use the following command.

Command	Mode	Description
no rule [NAME]	Global	Deletes a rule, enter a rule name optionally.

7.6.2.7 Displaying Rule

The following command can be used to show a certain rule by its name, all rules of a certain type, or all rules at once sorted by rule type.

Command	Mode	Description
show rule NAME	Enable Global	Shows a rule, enter a rule name. NAME: rule name
show rule		Shows all rules sorted by type.
show rule all		Shows all rules and admin access rules sorted by type.
show rule statistics		Shows rule statistics.
show rule-profile	Rule	Shows a current configuration of a rule.

The following is an example of configuring specific rule action on rule profile and showing it.

```
SWITCH# configure terminal
SWITCH(config)# rule jean create
SWITCH(config-rule[jean])# priority low
SWITCH(config-rule[jean])# match copy-to-cpu
SWITCH(config-rule[jean])# apply
SWITCH(config-rule[jean])# exit
SWITCH(config)# rule jean create
% Already exist rule
SWITCH(config)# show rule
rule jean
  priority low
  port any any
  match copy-to-cpu
SWITCH(config)# rule jean modify
SWITCH(config-rule[jean])no match copy-to-cpu
SWITCH(config-rule[jean]) show rule
rule jean
  priority low
  port any any
SWITCH(config-rule[jean])
```

7.6.3 QoS

For hiD 6610 S311, it is possible to use Strict Priority Queuing, Weighted Round Robin and Weighted Fair Queuing for a packet scheduling mode.

The following steps explain how QoS can be configured.

- Scheduling Algorithm
- Qos Weight
- Maximum and Minimum Bandwidth
- Random Early Discard (RED)
- Displaying QoS

7.6.3.1 Scheduling Algorithm

To process incoming packets by the queue scheduler, the hiD 6610 S311 provides the scheduling algorithm as Strict Priority Queuing (SP), Weighted Round Robin (WRR) and Weighted Fair Queuing (WFQ).

Weighted Round Robin (WRR)

WRR processes packets as much as weight. Processing the packets that have higher priority is the same way as strict priority queuing. However, it passes to next stage after processing as configured weight so that it is possible to configure for packet process not to be partial to the packets having higher priority. However, there is a limitation of providing differentiated service from those existing service.

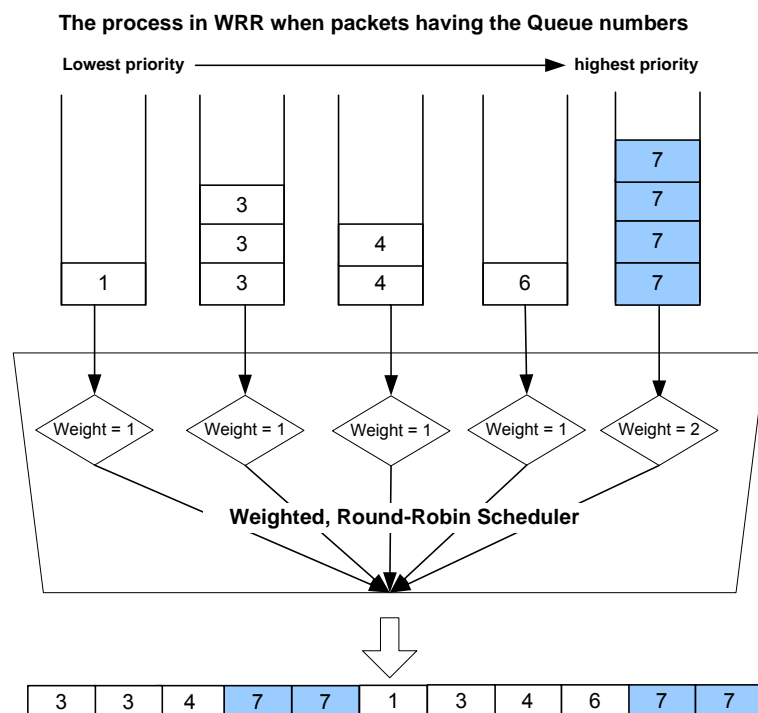


Fig. 7.1 Weighted Round Robin

Weighted Fair Queuing (WFQ)

Weighted fair queuing (WFQ) provides automatic sorting among individual traffic streams without requiring that you first define access lists. It can manage one way or two way streams of data: traffic between pairs of applications or voice and video.

In WFQ, packets are sorted in weighted order of arrival of the last bit, to determine transmission order. Using order of arrival of last bit emulates the behavior of Time Division Multiplexing (TDM), hence "fair"

From one point of view, the effect of this is that WFQ classifies sessions as high- or low-bandwidth. Low-bandwidth traffic gets priority, with high-bandwidth traffic sharing what's left over. If the traffic is bursting ahead of the rate at which the interface can transmit, new high-bandwidth traffic gets discarded after the configured or default congestive-messages threshold has been reached. However, low-bandwidth conversations, which include control-message conversations, continue to enqueue data.

Weighted Fair Queuing (WFQ)—Service According to Packet Finish Time

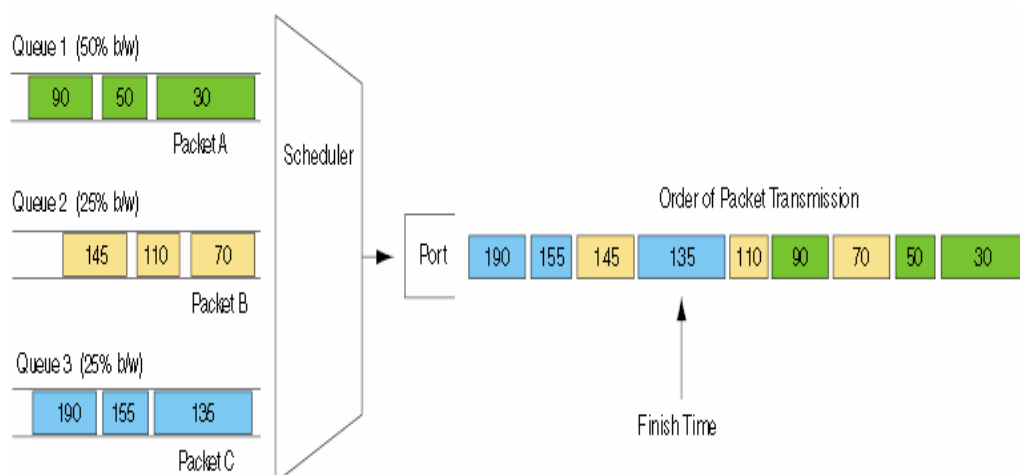


Fig. 7.2 Weighted Fair Queuing

Strict Priority Queuing (SP)

SPQ processes first more important data than the others. Since all data are processed by their priority, data with high priority can be processed fast but data without low priority might be delayed and piled up. This method has a strong point of providing the distinguished service with a simple way. However, if the packets having higher priority enter, the packets having lower priority are not processed.

The processing order in Strict Priority Queuing in case of entering packets having the Queue numbers as below

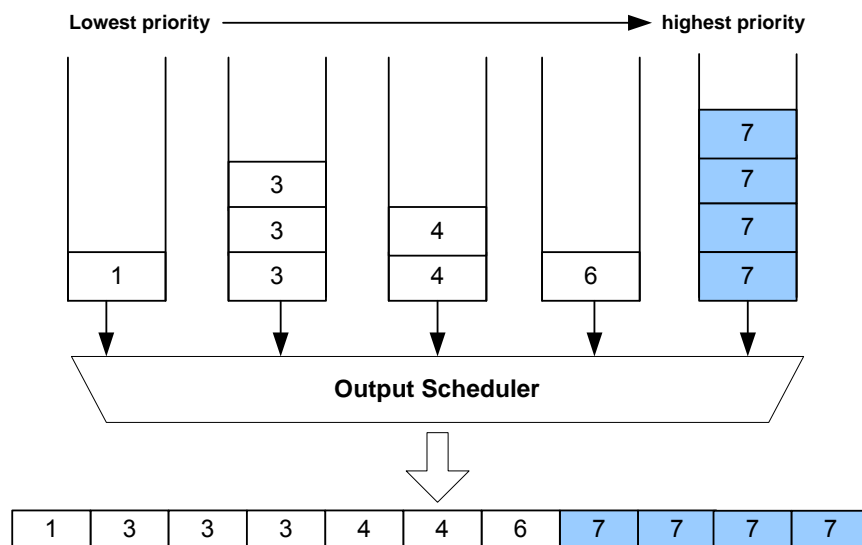


Fig. 7.3 Strict Priority Queuing

To select a packet scheduling mode, use the following command.

Command	Mode	Description
qos scheduling-mode {sp wrr wfq}	Global	Selects a packet scheduling mode for a ports: sp: strict priority queuing wrr: weighted round robin wfq: weighted fair queuing
qos cpu scheduling-mode {sp wrr}		Selects a scheduling mode for handling CPU packets sp: strict priority queuing wrr: weighted round robin



The default scheduling mode is **WRR**. And it is possible to assign a different scheduling mode to each port.

7.6.3.2 Qos Weight

To set a weight for WRR scheduling mode only, use the following command.

Command	Mode	Description
qos weight <i>PORTS</i> <0-7> {<1-15> unlimited }	Global	Sets a weight for each port and queue: PORTS: port numbers 0-7: queue number 1-15: weight value (default: 1) unlimited: strict priority queuing
qos cpu weight <0-7> {<1-15> unlimited }w		Sets a weight of CPU packet according to queue. 0-7: queue number 1-15: weight value (default: 1) unlimited: strict priority queuing

7.6.3.3 Maximum and Minimum Bandwidth

To set a maximum bandwidth, use the following command.

Command	Mode	Description
qos max-bandwidth <i>PORTS</i> <0-7> { <i>BANDWIDTH</i> unlimited }	Global	Sets a maximum bandwidth for each port and queue: PORTS: port numbers 0-7: queue number BANDWIDTH: bandwidth in the unit of MB unlimited: unlimited bandwidth



A maximum bandwidth can be set only in **WFQ** and **WRR** scheduling mode.

To set a maximum bandwidth, use the following command.

Command	Mode	Description
qos min-bandwidth <i>PORTS</i> <0-7> { <i>BANDWIDTH</i> unlimited }	Global	Sets a minimum bandwidth for each port and queue: PORTS: port numbers 0-7: queue number BANDWIDTH: bandwidth in the unit of MB (default: 0) unlimited: unlimited bandwidth



A minimum bandwidth can be set only in **WFQ** and **WRR** scheduling mode.

7.6.3.4 Random Early Discard (RED)

RED, which utilizes end-to-end flow-control of TCP, is a random packet dropping function when traffic reaches the user-designated threshold even before it reaches maximum buffer size. If traffic usage reaches maximum buffer size, all packets can be dropped, which makes packet loss. Therefore, in order to prevent packet loss or unstable traffic transmission, user can restrict excessive traffic over buffer size by setting up a threshold. With RED function, packet loss is reduced and stable packet transmission can be acquired. To apply RED function, RED function needs to be enabled.

To utilize RED function, start queue length value and drop probability are necessary. Start queue length represents the starting point of random packet dropping, and drop probability indicates the percentage of packet dropping from the starting point of random packet dropping to the point of complete dropping. If probability is large value, large amount of packets would be dropped. Therefore complete dropping point is slowly reached. On the other hand, if probability is little, little amount of packets would be dropped. Therefore complete dropping point is quickly reached. If the probability value is 1, dropping packet would be none and the value is 15, all packets would be dropped from the point of start queue length value is reached.

To enable/disable qos RED function in the system, use the following command.

Command	Mode	Description
qos red enable	Global	Enables RED function
qos red disable		Disables RED function.

To set up RED function by designating start threshold and probability, use the following command.

Command	Mode	Description
qos red <0-7> start <0-127> probability <1-15>	Global	Configures the value of parameters for RED operation. 0-7:cos number 0-127: start queue length value 1-15: drop probability
no qos red <0-7>		Deletes the configured parameter values.

7.6.3.5 Displaying QoS

To display a configuration of QoS, enter following command.

Command	Mode	Description
show qos	Enable Global	Shows a configuration of QoS for all ports.
show qos PORTS		Shows a configuration of QoS per each port.
show qos red		Shows a configuration of a RED function.
show qos cpu		Shows a configuration of QoS for CPU packets.

7.6.4 Admin Access Rule

For the hiD 6610 S311, it is possible to block a specific service connection like telnet, FTP, ICMP, etc with an admin access rule function.

7.6.4.1 Rule Creation

For the hiD 6610 S311, you need to open *Admin Access Rule Configuration* mode first. After opening *Admin Access Rule Configuration* mode, the prompt changes from SWITCH(config)# to SWITCH(config-admin-rule[NAME])#.

To open *Rule Configuration* mode, use the following command.

Command	Mode	Description
rule NAME create admin	Global	Opens <i>Admin Access Rule Configuration</i> mode, enter rule name.

After opening *Admin Access Rule Configuration* mode, a rule can be configured by user. The rule priority, packet classification and rule action(s) can be configured for each rule.



1. The rule name must be unique. Its size is limited to 63 significant characters.
2. The order in which the following configuration commands will be entered is arbitrary.
3. The configuration of a rule being configured can be changed as often as wanted (inclusive rule type) until the command, **apply**, will be entered.
4. Use the command, **show rule-profile**, to display the configuration entered up to now.

7.6.4.2 Rule Priority

If rules that are more than two match the same packet then the rule having a higher priority will be processed first.

To set a priority for an admin access rule, use the following command.

Command	Mode	Description
priority {low medium high highest}	Admin-rule	Sets a priority for a rule.



The default rule priority is **low** for an admin access rule.

7.6.4.3 Packet Classification

After configuring a packet classification for a rule, then configure how to process the packets. To specify a packet-classifying pattern, use the following command.



When specifying a source and destination IP address as a packet-classifying pattern, the destination IP address must be after the source IP address.

Command	Mode	Description
ip {A.B.C.D A.B.C.D/M any} {A.B.C.D A.B.C.D/M any} [0-255]	Admin-rule	Classifies an IP address: A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address 0-255: IP protocol number
ip {A.B.C.D A.B.C.D/M any} {A.B.C.D A.B.C.D/M any} icmp		Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address icmp: ICMP
ip {A.B.C.D A.B.C.D/M any} {A.B.C.D A.B.C.D/M any} icmp <0-255> any {<0-255> any}		Classifies an IP protocol (ICMP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address icmp: ICMP 0-255: ICMP message type number 0-255: ICMP message code number
ip {A.B.C.D A.B.C.D/M any} {A.B.C.D A.B.C.D/M any} {tcp udp}		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP udp: UDP
ip {A.B.C.D A.B.C.D/M any} {A.B.C.D A.B.C.D/M any} {tcp udp} {<1-65535> any} {<1-65535> any}		Classifies an IP protocol (TCP/UDP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP udp: UDP 0-65535: TCP/UDP source/destination port number any: any TCP/UDP source/destination port
ip {A.B.C.D A.B.C.D/M any} {A.B.C.D A.B.C.D/M any} tcp <0-65535> any {<0-65535> any} {TCP-FLAG any}		Classifies an IP protocol (TCP): A.B.C.D: source/destination IP address A.B.C.D/M: source/destination IP address with mask any: any source/destination IP address tcp: TCP 0-65535: TCP source/destination port number any: any TCP source/destination port TCP-FLAG: TCP flag (e.g. S(SYN), F(FIN)) any: any TCP flag

7.6.4.4 Rule Action

To specify a rule action (**match**) for the packets matching configured classifying patterns, use the following command.

Command	Mode	Description
match deny	Admin-rule	Denies a packet.
match permit		Permits a packet.

To delete a specified rule action (**match**), use the following command.

Command	Mode	Description
no match deny	Admin-rule	Deletes a specified rule action.
no match permit		

To specify a rule action (**no-match**) for the packets **not** matching configured classifying patterns, use the following command.

Command	Mode	Description
no-match deny	Admin-rule	Denies a packet.
no-match permit		Permits a packet.

To delete a specified rule action (**no-match**), use the following command.

Command	Mode	Description
no no-match deny	Admin-rule	Deletes a specified rule action.
no no-match permit		

7.6.4.5 Applying Rule

After configuring rule using the above commands, apply it to the system with the following command. If you do not apply a rule to the system, all specified rules will be lost.

To save and apply an admin access rule, use the following command.

Command	Mode	Description
apply	Admin-rule	Applies an admin access rule to the system.



1. The switch performs a detailed plausibility check and rejects the rule if the configuration is incomplete, contains bad or unsupported values or conflicts to other rules. In this case, the switch informs about the reason and the operator may correct the values
2. The switch may reject a rule with the message "% Already exist rule" although the name will not be listed by command, **show rule**. Unfortunately, the entered name in this case interferes with the name of an internally managed rule.
Remedy: Select another name for the rule (e.g. add a prefix).
3. All previously entered values remain valid after successful (or unsuccessful)

execution of command, **apply**. That is, if several rules being different only in one value should be created, then only the one changed value needs to be entered again.

7.6.4.6 Modifying and Deleting Rule

To modify a rule, use the following command.

Command	Mode	Description
rule <i>NAME</i> modify admin	Global	Modifies an admin access rule, enter a rule name.

To delete a rule, use the following command.

Command	Mode	Description
no rule admin	Global	Deletes an admin access rule, enter a rule name optionally.
no rule all		Deletes all rules and admin access rules.

7.6.4.7 Displaying Rule

The following command can be used to show a certain rule by its name, all rules of a certain type, or all rules at once sorted by rule type.

Command	Mode	Description
show rule admin	Enable Global	Shows all admin access rules sorted by type.
show rule all		Shows all rules and admin access rules sorted by type.
show rule statistics		Shows rule statistics.
show rule-profile	Admin-rule	Shows a current configuration of a rule.

7.7 NetBIOS Filtering

NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network (LAN). NetBIOS is used in Ethernet, included as part of NetBIOS Extended User Interface (NetBEUI). Resource and information in the same network can be shared with this protocol.

But the more computers are used recently, the more strong security is required. To secure individual customer's information and prevent information leakages in the LAN environment, the hiD 6610 S311 provides NetBIOS filtering function.

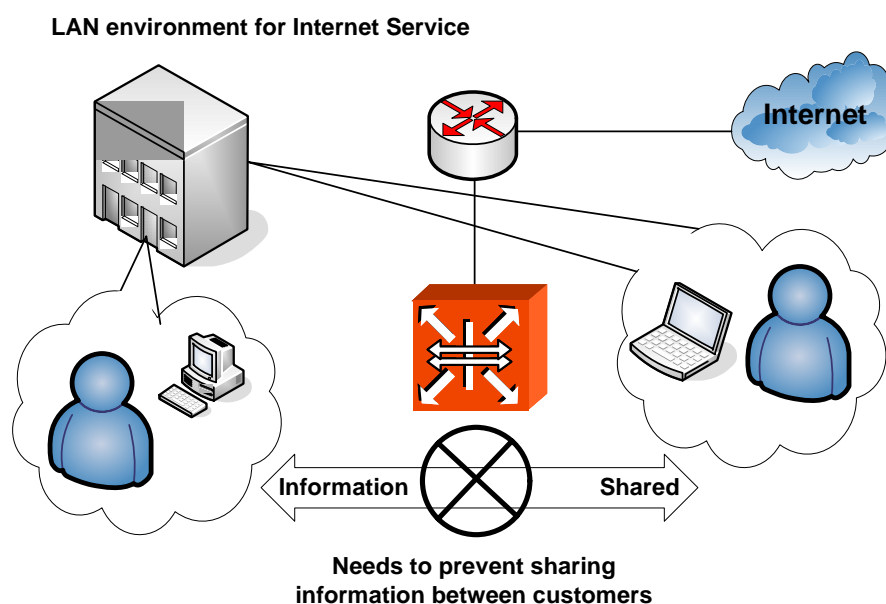


Fig. 7.4 NetBIOS Filtering

Without NetBIOS filtering, customer's data may be opened to each other even though the data should be kept. To keep customer's information and prevent sharing information in the above case, NetBIOS filtering is necessary.

Command	Mode	Description
netbios-filter <i>PORTS</i>	Bridge	Configures NetBIOS filtering to a specified port.

To disable NetBIOS filtering according to user's request, use the following command.

Command	Mode	Description
no netbios-filter <i>PORTS</i>	Bridge	Disables NetBIOS filtering from a specified port.

To display a configuration of NetBIOS filtering, use the following command.

Command	Mode	Description
show netbios-filter	Global Bridge	Shows a configuration of NetBIOS filtering.

The following is an example of configuring NetBIOS filtering in port 1~5 and showing it.

```
SWITCH(bridge)# netbios-filter 1-5
SWITCH(bridge)# show netbios-filter
o:enable .:disable
-----
          1          2
12345678901234567890123456|
-----
oooooooooooooooooooo
-----
SWITCH(bridge)#
```

7.8 Martian Filtering

It is possible to block packets, which trying to bring different source IP out from same network. If packet brings different IP address, not its source IP address, then it is impossible to know it makes a trouble. Therefore, you would better prevent this kind of packet outgoing from your network. This function is named as Martian filter.

To block packets which try to bring different source IP out from same network, use the following command.

Command	Mode	Description
ip martian-filter <i>INTERFACE</i>	Global	Blocks packets which bring different source IP address from specified interface. INTERFACE: enter the interface name.



It is not possible to configure both QoS and Martian filter at the same time.

To disable the configured Martian filter function, use the following command.

Command	Mode	Description
no ip martian-filter <i>INTERFACE</i>	Global	Disables a configured Martian filter function. INTERFACE: enter an interface name.



To see a configuration of Martian filter, use the **show running-config** command.

7.9 Max Host

You can limit the number of users by configuring maximum number of users also named as max hosts for each port. In this case, you need to consider not only the number of PCs in network but also devices such as switches in network.

For the hiD 6610 S311, you have to lock the port like MAC filtering before configuring max hosts. In case of ISPs, it is possible to arrange billing plan for each user by using this configuration.

To configure max host, use the following command.

Command	Mode	Description
max-hosts PORTS <1-16>	Bridge	Limits the number of connection to a port by setting maximum host: PORTS: enter the port number. 1-16: enter the maximum MAC number.
no max-hosts PORTS		Deletes configured max-host, enter the port number.

The following is an example of configuring to allow two MAC addresses to port 3, and five addresses to port 1, 2, and to ten addresses to port 7.

```
SWITCH(bridge)# max-hosts 3 2
SWITCH(bridge)# max-hosts 1 5
SWITCH(bridge)# max-hosts 2 5
SWITCH(bridge)# max-hosts 7 10
SWITCH(bridge)#
```

To display configured max host, use the following command.

Command	Mode	Description
show max-hosts	Enable Global Bridge	Shows configured max host.

The following is an example of displaying configured max hosts.

```
SWITCH(bridge)# show max-hosts
port 1 :      0/5      (current/max)
port 2 :      0/5      (current/max)
port 3 :      0/2      (current/max)
port 4 :      0/Unlimited (current/max)
port 5 :      0/Unlimited (current/max)
port 6 :      0/Unlimited (current/max)
port 7 :      0/10     (current/max)
port 8 :      0/Unlimited (current/max)
port 9 :      0/Unlimited (current/max)
port 10 :     0/Unlimited (current/max)
```

7.9.1 Max New Hosts

Max-new-hosts feature is to limit the number of users by configuring the number of MAC address that can be learned on the system and on the port for a second. The number of MAC address that can be learned on the system has the priority.

To configure max new hosts, use the following command.

Command	Mode	Description
max-new-hosts <i>PORTS</i> <i>MAX-MAC-NUMBER</i>	Bridge	The number of MAC address that can be learned on the port for a second.
max-new-hosts system <i>PORTS</i> <i>MAX-MAC-NUMBER</i>		The number of MAC address that can be learned on the system for a second.

To delete configured max new hosts, use the following command.

Command	Mode	Description
no max-new-hosts <i>PORTS</i>	Bridge	Deletes the number of MAC address that can be learned on the port.
no max-new-hosts system		Deletes the number of MAC address that can be learned on the system.

To display configured max new hosts, use the following command.

Command	Mode	Description
show max-new-hosts	Enable Global Bridge	Shows the configured Max-new-hosts.

If MAC that already counted disappears before passing 1 second and starts learning again, it is not counted. In case the same MAC is detected on the other port also, it is not counted again. For example, if MAC that was learned on port 1 is detected on port 2, it is supposed that MAC moved to the port 2. So, it is deleted from the port 1 and learned on the port 2 but it is not counted.

7.10 Port Security

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the PCs that are allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the PC attached to that port is assured the full bandwidth of the port.

7.10.1 Port Security on Port

Step 1

Enable port security on the port.

Command	Mode	Description
port security <i>PORTS</i>	Bridge	Enables port security on the port. PORT: selects port number

Step 2

Set the maximum number of secure MAC address for the port.

Command	Mode	Description
port security <i>PORTS</i> maximum <i><1-16384></i>	Bridge	Sets a maximum number of secure MAC address for the port. 1-16384: Maximum number of addresses (default: 1)

Step 3

Set the violation mode and the action to be taken.

Command	Mode	Description
port security <i>PORTS</i> violation <i>{shutdown protect restrict}</i>	Bridge	Selects a violation mode.

When configuring port security, note that the following information about port security violation modes:

- **protect** drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
- **restrict** drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the Security Violation counter to increment.
- **shutdown** puts the interface into the error-disabled state immediately and sends an SNMP trap notification

Step 4

Enter a secure MAC address for the port.

Command	Mode	Description
port security <i>PORTS</i> mac-address <i>MACADDR</i> vlan <i>NAME</i>	Bridge	Sets a secure MAC address for the port. PORTS: select the port number. MACADDR: enter the MAC address. NAME: vlan name

To disable the configuration of port secure, use the following command.

Command	Mode	Description
no port security <i>PORTS</i>	Bridge	Disables port security on the port.
no port security <i>PORTS</i> mac-address <i>MACADDR</i> vlan <i>NAME</i>		Deletes a secure MAC address for the port. PORTS: enter the port number MACADDR: enter the MAC address.
no port security <i>PORTS</i> maximum		Returns to the default number of secure MAC address. (default: 1)
no port security <i>PORTS</i> violation		Returns to the violation mode to the default. (shutdown mode)

To display the configuration of port security, use the following command.

Command	Mode	Description
show port security [<i>PORTS</i>]	Bridge	Shows port security on the port.

This is an example of configuring port security on port 7.

```
SWITCH(config)# bridge
SWITCH(bridge)# port security 7
SWITCH(bridge)# port security 7 maximum 10000
SWITCH(bridge)# port security 7 violation protect
SWITCH(bridge)# port security 7 mac-address 00:02:a5:74:9b:17 vlan 1
SWITCH(bridge)# show port security 7
=====
port security violation aging   type      static  maximum current
=====
  7  enabled  protect    -  absolute    -   10000      1

=====

port   vlan   secure-mac-addr      status    in use
=====
  7      1    00:02:a5:74:9b:17    static      -

SWITCH(bridge)# no port security 7 maximum
SWITCH(bridge)# no port security 7 violation
SWITCH(bridge)# show port security 7
```

```

=====
port security violation aging type static maximum current
=====
7 enabled shutdown - absolute - 1 0

=====
port vlan secure-mac-addr status in use
=====
SWITCH(bridge)#

```

7.10.2 Port Security Aging

Port security aging is to set the aging time for all secure addresses on a port. Use this feature to remove and add PCs on a secure port without manually deleting the existing secure MAC addresses while still limiting the number of secure addresses on a port.

Command	Mode	Description
port security <i>PORTS</i> aging static	Bridge	Enables aging for configured secure addresses.
port security <i>PORTS</i> aging time <1-1440>		Configures aging time in minutes for the port. All the secure addresses age out exactly after the time.
port security <i>PORTS</i> aging type {absolute inactivity}		Configures aging type.

- **absolute** all the secure addresses on this port age out exactly after the time (minutes) specified lapses and are removed from the secure address list.
- **inactivity** the secure addresses on this port age out only if there is no data traffic from the secure source addresses for the specified time period.

To disable the configuration of port secure aging, use the following command.

Command	Mode	Description
no port security <i>PORTS</i> aging static	Bridge	Disables aging for only statistically configured secure addresses.
no port security <i>PORTS</i> aging time		Disables port secure aging for all secure addresses on a port.
no port security <i>PORTS</i> aging type		Returns to the default condition. (absolute)

To display the configuration of port security, use the following command.

Command	Mode	Description
show port security [<i>PORTS</i>]	Enable Global Bridge	Shows port security on the port.

7.11 MAC Table

A dynamic MAC address is automatically registered in the MAC table, and it is removed if there is no access to/from the network element corresponding to the MAC address during the specified MAC aging time. On the other hand, a static MAC address is manually registered by user. This will not be removed regardless of the MAC aging time before removing it manually.

To manage MAC table in the switch, use the following command.

Command	Mode	Description
mac <i>NAME PORT MACADDR</i>	Bridge	Specifies a static MAC address in the MAC table. NAME: enter the bridge name. PORT: enter the port number. MACADDR: enter the MAC address.
mac aging-time <10-21474830>		Specifies MAC aging time: 10-21474830: aging time (default: 300)

To remove registered dynamic MAC addresses from the MAC table, use the following command.

Command	Mode	Description
clear mac	Enable Global Bridge	Clears dynamic MAC addresses.
clear mac <i>NAME</i>		Clears dynamic MAC addresses.
clear mac <i>NAME PORT</i>		Clears dynamic MAC addresses. NAME: enter the bridge name. PORT: enter the port number.
clear mac <i>NAME PORT MACADDR</i>		Clears dynamic MAC addresses. NAME: enter the bridge name. PORT: enter the port number. MACADDR: enter the MAC address.

To remove static MAC addresses manually registered by user from the MAC table, use the following command.

Command	Mode	Description
no mac	Bridge	Deletes static MAC addresses.
no mac <i>NAME</i>		Deletes static MAC addresses, enter the bridge name.
no mac <i>NAME PORT</i>		Deletes static MAC addresses. NAME: enter the bridge name. PORT: enter the port number.
no mac <i>NAME PORT MACADDR</i>		Deletes a specified static MAC address. NAME: enter the bridge name. PORT: enter the port number. MACADDR: enter the MAC address.

To display a MAC table in the switch, use the following command.

Command	Mode	Description
show mac <i>NAME</i> [<i>PORT</i>]	Enable Global Bridge	Shows switch MAC address, selection by port number (subscriber port only): NAME: enter the bridge name PORT: select the port number.



There are more than a thousand of MAC addresses in MAC table. And it is difficult to find information you need at one sight. So, the system shows certain amount of addresses displaying **—more—** on standby status. Press any key to search more. After you find the information, you can go back to the system prompt without displaying the other table by pressing **<q>**.

7.12 MAC Filtering

It is possible to forward frame to MAC address of destination. Without specific performance degradation, maximum 4,096 MAC addresses can be registered.

7.12.1 Default Policy of MAC Filtering

The basic policy of filtering based on system is set to allow all packets for each port. However the basic policy can be changed for user's requests.

After configuring basic policy of filtering for all packets, use the following command on Bridge mode to show the configuration.

Command	Mode	Description
mac-filter default-policy {deny permit} <i>PORTS</i>	Bridge	Configures basic policy of MAC Filtering in specified port.

By default, basic filtering policy provided by system is configured to permit all packets in each port.

Sample Configuration

This is an example of blocking all packets in port 1~3 and port 7.

```
SWTICH(bridge)# mac-filter default-policy deny 5-10
SWTICH(bridge)# mac-filter default-policy permit 2
SWTICH(bridge)# show mac-filter default-policy
```

```
-----
PORT POLICY | PORT POLICY
-----+-----
1 PERMIT | 2 PERMIT
3 PERMIT | 4 PERMIT
5 DENY | 6 DENY
7 DENY | 8 DENY
9 DENY | 10 DENY
-----
```



```

11 PERMIT | 12 PERMIT
13 PERMIT | 14 PERMIT
15 PERMIT | 16 PERMIT
17 PERMIT | 18 PERMIT
19 PERMIT | 20 PERMIT
21 PERMIT | 22 PERMIT
23 PERMIT | 24 PERMIT
25 PERMIT | 26 PERMIT
27 PERMIT | 28 PERMIT
SWITCH(bridge)#

```

7.12.2 Adding Policy of MAC Filter

You can add the policy to block or to allow some packets of specific address after configuring the basic policy of MAC Filtering. To add this policy, use the following commands on *Bridge Configuration* mode.

Command	Mode	Description
mac-filter add <i>MACADDR</i> {deny permit}	Bridge	Allows or blocks packet which brings configured mac address to specified port.

Variable MAC-ADDRESS is composed of twelve digits number in Hexa decimal. It is possible to check it by using the **show mac** command. 00:d0:cb:06:01:32 is an example of MAC address.

7.12.3 Deleting MAC Filter Policy

To delete MAC filtering policy, use the following command.

Command	Mode	Description
mac-filter del <i>SOURCE-MACADDR</i>	Bridge	Deletes filtering policy for specified MAC address.

To delete MAC filtering function, use the following command.

Command	Mode	Description
no mac-filter	Bridge	Deletes all MAC filtering functions.

7.12.4 Listing of MAC Filter Policy

If you need to make many MAC filtering policies at a time, it is hard to input command one by one. In this case, it is more convenient to save MAC filtering policies at “/etc/mfdb.conf” and display the list of MAC filtering policy. To view the list of MAC filtering policy at /etc/mfdb.conf, use the following command.

Command	Mode	Description
mac-filter list	Bridge	Shows the list of MAC filtering policy at /etc/mfdb.conf.

7.12.5 Displaying MAC Filter Policy

To show a configuration about MAC filter policy, use the following command.

Command	Mode	Description
show mac-filter default-policy	Enable / Global / Bridge	Shows MAC filter policy.
show mac-filter		
show mac-filter COUNT		
show mac-filter COUNT SOURCE-MACADDR		

Sample Configuration

The latest policy is recorded as number 1. The following is an example of permitting MAC address 00:02:a5:74:9b:17 and 00:01:a7:70:01:d2 and showing table of filter policy.

```
SWITCH(bridge)# mac-filter add 00:02:a5:74:9b:17 permit
SWITCH(bridge)# mac-filter add 00:01:a7:70:01:d2 permit
SWITCH(bridge)# show mac-filter
=====
ID |          MAC          | ACTION
=====
  1  00:01:a7:70:01:d2   PERMIT
  2  00:02:a5:74:9b:17   PERMIT
SWITCH(bridge)#
```

The following is an example of displaying one configuration.

```
SWITCH(bridge)# show mac-filter 1
=====
ID |          MAC          | ACTION
=====
  1  00:01:a7:70:01:d2   PERMIT
SWITCH(bridge)#
```

7.13 Address Resolution Protocol (ARP)

Device connected to IP network has two addresses, LAN address and network address. LAN address is sometimes called as data link because it is used in Layer 2 level, but more commonly the address is known as MAC address. Ethernet Switch needs 48-bit-MAC address to transmit packets. In this case, the process of finding proper MAC address from IP address is called as address resolution.

On the other hand, the progress of finding proper IP address from MAC address is called as reverse address resolution. Siemens switches find MAC address from IP address through address resolution protocol (ARP).

This chapter consists of these sections:

- ARP Table
- ARP Alias
- ARP-Inspection
- Gratuitous ARP

7.13.1 ARP Table

Hosts typically have an ARP table, which is a cache of IP/MAC address mappings. The ARP Table automatically maps the IP address to the MAC address of a switch. In addition to address information, the table shows the age of the entry in the table, the encapsulation method, and the switch interface (VLAN ID) where packets are forwarded.

The hiD 6610 ARP saves IP/MAC addresses mappings in ARP table for quick search. Referring to the information in ARP table, packets attached IP address is transmitted to network. When configuring ARP table, it is possible to do it only in some specific interfaces.

7.13.1.1 Registering ARP Table

The contents of ARP table are automatically registered when MAC address corresponds to MAC address is founded. The network administrator could use MAC address of specific IP address in Network by registering on ARP table.

To make specific IP address to be accorded with MAC address, use the following command.

Command	Mode	Description
arp A.B.C.D MACADDR	Global	Sets a static ARP entry, enter the IP address and the MAC address. MACADDR: enter the MAC address.
arp A.B.C.D MACADDR INTER-FACE		Sets a static ARP entry, enter the IP address, the MAC address and enter an interface name. INTERFACE: enter an interface name. MACADDR: enter the MAC address.

To delete registered IP address and MAC address or change all the contents of ARP table, use one of the following command.

Command	Mode	Description
no arp <i>A.B.C.D</i>	Global	Negates a command or set sets its default, enter the IP address.
no arp <i>A.B.C.D INTERFACE</i>		Negates a command or set sets its default, enter the IP address and enter the interface name.
clear arp	Enable	Deletes all the contents of ARP table.
clear arp <i>INTERFACE</i>	Global	Deletes all the contents of ARP table, enter the interface name.

7.13.1.2 Displaying ARP Table

To display ARP table registered in switch, use one of the following command.

Command	Mode	Description
show arp	Enable Global	Shows ARP table.
show arp { <i>INTERFACE</i> <i>A.B.C.D</i> }		Shows ARP table for specified interface, enter the interface name or IP address. (br1, br2, ...).

The following is an example of registering 10.1.1.1 as IP address and 00:d0:cb:00:00:01 as MAC address. This command displays ARP table.

```
SWITCH(config)# arp 10.1.1.1 00:d0:cb:00:00:01
SWITCH(config)# show arp
```

Address	HWaddress	Type	Interface
10.254.254.105	00:bb:cc:dd:ee:05	DYNAMIC	br4094
10.2.2.1	00:00:cd:01:82:d0	DYNAMIC	br2

```
SWITCH(config)#
```

7.13.2 ARP Alias

Although clients are joined in same client switch, it may be impossible to communicate between clients for their private security. When you need to make them communicate each other, the hiD 6610 S311 supports ARP alias, which responses ARP request from client net through concentrating switch.

To register address of client net range in ARP alias, use the following command.

Command	Mode	Description
arp-alias <i>A.B.C.D A.B.C.D</i> [<i>MACADDR</i>]	Global	Registers IP address range and MAC address in ARP alias to make user's equipment response ARP request.



Unless you input MAC address, MAC address of user's equipment will be used for ARP response.

To delete registered IP address range of ARP alias, use the following command.

Command	Mode	Description
no arp-alias <i>START-IP-ADDRESS</i> <i>END-IP-ADDRESS</i>	Global	Deletes a registered IP address range of ARP alias.

To display ARP alias, use the following command.

Command	Mode	Description
show arp-alias	Enable Global	Shows a registered ARP alias.

7.13.3 ARP-Inspection

ARP provides IP communication by mapping an IP address to a MAC address. However, a malicious user can attack ARP caches of systems by intercepting the traffic intended for other hosts on the subnet. For example, Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. If Host C responds with an IP address of Host A (or B) and a MAC address of Host C, Host A and Host B can use Host C's MAC address as the destination MAC address for traffic intended for Host A and Host B.

ARP Inspection is a security feature that validates ARP packets in a network. It discards ARP packets with invalid IP-MAC address binding.

7.13.3.1 Enabling ARP Inspection

To enable and disable ARP Inspection on the hiD 6610 S311 system, use the following command.

Command	Mode	Description
arp-inspection enable	Global	Enables ARP-inspection function.
arp-inspection disable		Disables ARP-inspection function.

7.13.3.2 ARP Inspection mapping policy

You can configure the policy to permit or deny ARP packets by **arp-inspection mapping** command.

Command	Mode	Description
arp-inspection mapping { <i>A.B.C.D</i> <i>A.B.C.D/M</i> <i>any</i> } { <i>MACADDR</i> <i>any</i> } permit	Global	Configures the policy to permit ARP packets when they meet the requirements. A.B.C.D: IP-Address for inspection MACADDR: Mac-Address
arp-inspection mapping { <i>A.B.C.D</i> <i>A.B.C.D/M</i> <i>any</i> } { <i>MACADDR</i> <i>any</i> } deny		Configures the policy to deny ARP packets when they meet the requirements. A.B.C.D: IP-Address for inspection

To remove the policy of ARP packets, use the following command.

Command	Mode	Description
no arp-inspection mapping {A.B.C.D A.B.C.D/M any} {MACADDR any}	Global	Deletes the configured policy of ARP packets for specified condition.
no arp-inspection mapping all		Deletes the configured policy of ARP packets for all conditions.

7.13.3.3 Configuring IP address-validation

If arp-inspection address-validation function is enabled, hiD 6610 S311 drops ARP packets in the following cases.

- If ARP Request packet's IP-address is 0.0.0.0 or 255.255.255.255, these ARP Request packets are dropped.
- If ARP Reply packets; source IP address is 0.0.0.0 or 255.255.255.255, these ARP Reply packets are dropped.

You can configure the switch to perform additional checks on the destination MAC address, the sender and target IP address and the source MAC address.

Command	Mode	Description
arp-inspection address-validation enable	Global	Inspects specific check on incoming ARP packets.

To remove the specific ARP Inspection configuration, use the following commands

Command	Mode	Description
arp-inspection address-validation disable	Global	Removes specific ARP inspection configuration.

7.13.3.4 Enabling match-mac

If arp-inspection match-mac function is enabled, hiD 6610 S311 drops ARP packets in the following cases.

- When ARP Reply/Request packet's source mac-address is not consistent with mac-address of the subject which has been sent this ARP Reply packet.
- When ARP Reply packet's destination mac-address is not consistent with mac-address of the destination which will be received this ARP packet.

To enable/disable the function to permit the right packets only when they have the proper mac-address, use the following command.

Command	Mode	Description
arp-inspection match-mac enable	Global	Enables match-mac function
arp-inspection match-mac disable		Disables match-mac function.

7.13.3.5 Displaying ARP Inspection

To display checking and statistics, use the **show arp-inspection** command in *Global Configuration* mode.

Command	Mode	Description
show arp-inspection mapping	Enable Global	Displays the information of ARP inspection.
show arp-inspection statistics		
show arp-inspection status		

You can clear ARP-Inspection mapping counter and statistics using the following command.

Command	Mode	Description
clear arp-inspection {statistics mapping counter}	Enable Global	Clears ARP-Inspection statistics or mapping counts.

[Sample Configuration]

The following is an example of configuring to drop or permit the ARP Request and Reply packets according to their MAC-address and IP address inspection.

```
SWITCH(config)# arp-inspection enable
SWITCH(config)# arp-inspection mapping 10.1.1.1/32 00:00:01:00:00:01 deny
SWITCH(config)# arp-inspection mapping any 00:00:01:00:00:01 permit
SWITCH(config)# arp-inspection mapping 10.1.1.0/27 any deny
SWITCH(config)# show arp-inspection mapping
```

```
-----
                        ARP Inspection Mapping
-----
```

IP	MAC	Action	Counter
10.1.1.1/32	00:00:01:00:00:01	deny	0
any	00:00:01:00:00:01	permit	0
10.1.1.0/27	any	deny	0

```
SWITCH(config)#
```

7.13.4 Gratuitous ARP

Gratuitous ARP is a broadcast packet like an ARP request. It containing IP address and MAC address of gateway, and the network is accessible even though IP addresses of specific host's gateway are repeatedly assigned to the other.

Configure Gratuitous ARP interval and transmission count using following commands. And configure transmission delivery-start in order to transmit Gratuitous ARP after ARP reply.

Gratuitous ARP is transmitted after some time from transmitting ARP reply.

Command	Mode	Description
arp-patrol <i>TIME COUNT</i> [<i>TIME</i>]	Global	Configures a gratuitous ARP. TIME: transmit interval COUNT: transmit count
no arp-patrol		Disables a gratuitous ARP.

The following is an example of configuring the transmission interval as 10 sec and transmission times as 4 and showing it.

```
SWITCH(config)# arp-patrol 10 4
SWITCH(config)# show running-config
Building configuration...
Current configuration:
hostname SWITCH
(Omitted)
arp-patrol 10 4
!
no snmp
!
SWITCH(config)#
```

7.13.5 Proxy-ARP

To configure Proxy-ARP, you need to enter *Interface configuration* mode and use the following command.

Command	Mode	Description
ip proxy-arp	Interface	Sets proxy-ARP at specified Interface
no ip proxy-arp		Removes the configured proxy-ARP from the interface.

7.14 ICMP Message Control

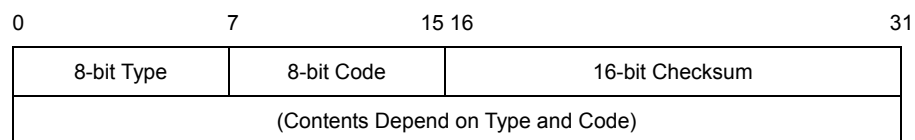
ICMP stands for Internet Control Message Protocol. When it is impossible to transmit data or configure route for data, ICMP sends error message about it to host. The first 4 bytes of all ICMP messages are same, but the other parts are different according to type field value and code field value. There are fifteen values of field to distinguish each different ICMP message, and code field value helps to distinguish each type in detail.

The following table shows explanation for fifteen values of ICMP message type.

Type	Value	Type	Value
ICMP_ECHOREPLY	0	ICMP_DEST_UNREACH	3
ICMP_SOURCE_QUENCH	4	ICMP_REDIRECT	5
ICMP_ECHO	8	ICMP_TIME_EXCEEDED	11
ICMP_PARAMETERPROB	12	ICMP_TIMESTAMP	13
ICMP_TIMESTAMPREPLY	14	ICMP_INFO_REQUEST	15
ICMP_INFO_REPLY	16	ICMP_ADDRESS	17
ICMP_ADDRESSREPLY	18		

Tab. 7.1 ICMP Message Type

The following figure shows simple ICMP message construction.



It is possible to control ICMP message through user's configuration. You can configure to block the echo reply message to the partner who is doing ping test to device and interval to transmit ICMP message.

7.14.1 Blocking Echo Reply Message

It is possible to configure block echo reply message to the partner who is doing ping test to switch. To block echo reply message, use the following commands.

Command	Mode	Description
ip icmp ignore echo all	Global	Blocks echo reply message to all partners who are taking ping test to device.
ip icmp ignore echo broadcast		Blocks echo reply message to partner who is taking broadcast ping test to device.

To release the blocked echo reply message, use the following commands.

Command	Mode	Description
no ip icmp ignore echo all	Global	Releases blocked echo reply message to all partners who are taking ping test to device.
no ip icmp ignore echo broadcast		Releases blocked echo reply message to partner who is taking broadcast ping test to device.

7.14.2 Interval for Transmit ICMP Message

User can configure the interval for transmit ICMP message. After you configure the interval, ICMP message will be blocked until the period based on the last message is up. For example, if you configure the interval as 1 second, ICMP will not be sent within 1 second after the last message has been sent.

To configure interval to transmit ICMP message, the administrator should configure the type of message and the interval time.

Use the following command, to configure the interval for transmit ICMP message.

Command	Mode	Description
ip icmp interval rate-mask MASK	Global	Configures the interval for transmit ICMP message. MASK: user should input hexadecimal value until 0xFFFFFFFF. The default is 0x1818.

If mask that is input as hexadecimal number is calculated as binary number “1” means “Status ON”, “0” means “Status OFF”. In binary number, if the digit showed as “1” matches with the value of ICMP message. It means ICMP Message is selected as “Status ON”. Digit value starts from 0.

For example, if hexadecimal number “8” is changed as binary number, it is “1000”. In 1000, 0 digit is “0” and 1 digit is “0”, 2 digit is “0” and 3 digit is “1”. The digit showed as “1” is “3” and ICMP_DEST_UNREACH means ICMP value is “3”. Therefore, ICMP_DEST_UNREACH is chosen the message of limiting the transmission time.

Default is 0x1818. If 1818 as hexadecimal number is changed as binary number, it is 1100000011000. By calculating from 0 digit, 3 digit, 4 digit, 11 digit, 12 digit is “1” and it is “STATUS ON”. Therefore, the message that corresponds to 3, 4, 11, and 12 is chosen as the message limiting the transmission rate.

Tab. 7.2 shows the result of mask calculation of default value.

Type	Status
ICMP_ECHOREPLY (0)	OFF
ICMP_DEST_UNREACH (3)	ON
ICMP_SOURCE_QUENCH (4)	ON
ICMP_REDIRECT (5)	OFF
ICMP_ECHO (8)	OFF
ICMP_TIME_EXCEEDED (11)	ON
ICMP_PARAMETERPROB (12)	ON
ICMP_TIMESTAMP (13)	OFF
ICMP_TIMESTAMPREPLY (14)	OFF
ICMP_INFO_REQUEST (15)	OFF
ICMP_INFO_REPLY (16)	OFF
ICMP_ADDRESS (17)	OFF
ICMP_ADDRESSREPLY (18)	OFF

Tab. 7.2 Mask Calculation of Default Value

To configure the limited ICMP transmission time, use the following command.

Command	Mode	Description
ip icmp interval rate-limit <i>INTERVAL</i>	Global	Configures a limited ICMP transmission time. INTERVAL: 0-2000000000 (unit: 10 ms)



The default ICMP interval is 1 second (100 ms).

To return to default ICMP configuration, use the following command.

Command	Mode	Description
ip icmp interval default	Global	Returns to default configuration.

To display ICMP interval configuration, use the following command.

Command	Mode	Description
show ip icmp interval	Enable Global	Shows ICMP interval configuration.

7.14.3 The policy of unreachable messages

When the packets can't reach Destination host or the network, the switch is supposed to bring them back to the source IP address. What if too many unreachable packets are coming into the system, it might cause slow down the system operation.

Not to bring these messages back to source IP address on a specific interface, use the following command on *Interface Configuration* mode.

Command	Mode	Description
ip unreachable	Interface	Configures not to bring unreachable messages back to their source IP address on interface.
no ip unreachable		Brings all unreachable messages back to their source IP address on interface.

7.15 IP TCP Flag Control

TCP (Transmission Control Protocol) header includes six kinds of flags that are URG, ACK, PSH, RST, SYN, and FIN. For the hiD 6610 S311, you can configure RST and SYN as the below.

7.15.1 RST Configuration

RST sends a message when TCP connection can not be done to a person who tries to make it. However, it is also possible to configure to block the message. This function will help prevent that hackers can find impossible connections.

To configure not to send the message that informs TCP connection can not be done, use the following command.

Command	Mode	Description
ip tcp ignore rst-unknown	Global	Configures to block the message that informs TCP connection can not be done.
no ip tcp ignore rst-unknown		Responds the message again that informs TCP connection is not possible.

7.15.2 SYN Configuration

SYN sets up TCP connection. The hiD 6610 S311 transmits cookies with SYN to a person who tries to make TCP connection. And only when transmitted cookies are returned, it is possible to permit TCP connection. This function prevents connection overcrowding because of accessed users who are not using and helps the other users use service.

To permit connection only when transmitted cookies are returned after sending cookies with SYN, use the following command.

Command	Mode	Description
ip tcp syncookies	Global	Permits only when transmitted cookies are returned after sending cookies with SYN.
no ip tcp syncookies		Disables configuration to permit only when transmitted cookies are returned after sending cookies with SYN.

7.16 Packet Dump

Failures in network can occur by certain symptom. Each symptom can trace to one or more problems by using specific troubleshooting tools. The hiD 6610 S311 switch provides the debug command to dump packet. Use debug commands only for problem isolation. Do not use it to monitor normal network operation. The debug commands produce a large amount of processor overhead.

7.16.1 Verifying Packet Dump

You can configure a packet dump type to verify dumped packets as the follows.

- Packet Dump by Protocol
- Packet Dump with Option

The hiD 6610 S311 also provides debug command for Layer 3 routing protocols (BGP, OSPF, RIP and PIM). If you want to debug about them, refer to the each configuration chapter.

7.16.1.1 Packet Dump by Protocol

You can see packets about BOOTPS, DHCP, ARP and ICMP using the following command.

Command	Mode	Description
debug packet { <i>interface</i> <i>INTER-FACE</i> <i>port</i> <i>PORTS</i> } protocol { <i>bootps</i> <i>dhcp</i> <i>arp</i> <i>icmp</i> } { <i>src-ip</i> <i>A.B.C.D</i> <i>dest-ip</i> <i>A.B.C.D</i> }	Enable	Shows packet dump by protocol.
debug packet { <i>interface</i> <i>INTER-FACE</i> <i>port</i> <i>PORTS</i> } host { <i>src-ip</i> <i>A.B.C.D</i> <i>dest-ip</i> <i>A.B.C.D</i> } { <i>src-port</i> <1-65535> <i>dest-port</i> <1-65535>}		Shows host packet dump.
debug packet { <i>interface</i> <i>INTER-FACE</i> <i>port</i> <i>PORTS</i> } multicast { <i>src-ip</i> <i>A.B.C.D</i> <i>dest-ip</i> <i>A.B.C.D</i> }		Shows multicast packet dump.
debug packet { <i>interface</i> <i>INTER-FACE</i> <i>port</i> <i>PORTS</i> } src-ip <i>A.B.C.D</i> <i>dest-ip</i> <i>A.B.C.D</i> }		Show packet dump by source IP address or destination IP address.
debug packet { <i>interface</i> <i>INTER-FACE</i> <i>port</i> <i>PORTS</i> } dest-ip <i>A.B.C.D</i>		

7.16.1.2 Packet Dump with Option

You can verify packets with TCP dump options using the following command.

Command	Mode	Description
debug packet <i>OPTION</i>	Enable	Shows packet dump using options.

Tab. 7.3 shows the options for packet dump.

Option	Description
-a	Change Network & Broadcast address to name.
-d	Change the complied packet-matching code to readable letters and close it
-e	Output link-level header of each line
-f	Output outer internet address as symbol
-l	Buffer output data in line. This is useful when other application tries to receive data from tcpdump.
-n	Do not translate all address (e.g. port, host address)
-N	When output host name, do not print domain.
-O	Do not run packet-matching code optimizer. This option is used to find bug in optimizer
-p	Interface is not remained in promiscuous mode
-q	Reduce output quantity of protocol information. Therefore, output line is shorter.
-S	Output TCP sequence number not relative but absolute
-t	Time is not displayed on each output line
-v	Display more information
-w	Save the captured packets in a file instead of output
-x	Display each packet as hexacode
-c NUMBER	Close the debug after receive packets as many as the number
-F FILE	Recieves file as filter expression. All additional expressions on command line are ignored.
-i INTERFACE	Desinate the interface where the intended packets are transmitted. If not designated, it automatically select a interface which has the lowest number within the system interfaces (Loopback is excepted)
-r FILE	Read packets from the file which created by '-w' option.
-s SNAPLEN	This is used to configure sample packet except the 68 byte default value. The 68 byte is appropriate value for IP, ICMP, TCP and UDP, but it can truncate protocol information of Name server or NFS packets. If sample size is long, the system should take more time to inspect and packets can be dropped for small buffer size. On the contrary, if the sample size is small, information can be leaked as the amount. Therefore, user should adjust the size as header size of protocol.
-T TYPE	Display the selected packets by conditional expression as the intended type. rpc (Remote Procedure Call) rtp (Real-time Transport Protocol) rtcp (Real-time Transport Control Protocol) vat (Visual Audio Tool) wb (distributed White Board)
EXPRESSION	Conditional expression

Tab. 7.3 Options for Packet Dump

7.16.2 Debug Packet Dump

The hiD 6610 S311 provides network debugging function to prevent system overhead for unknown packet inflow. Monitoring process checks CPU load per 5 seconds. If there is more traffic than threshold, user can capture packets using TCP Dump and save it to file. User can download the dump file with the name of file-number.dump after FP connection to the system. Verify the dumped packet contents with a packet analyze program.

To debug packet dump, use the following command.

Command	Mode	Description
debug packet log <i>COUNT</i> <i>VALUE TIME</i> [1-10]	Enable	Debug with according to the conditions COUNT: packet counting VALUE: CPU-threshold 1-10: file number
no debug packet log		Release the debug configuration



Basically, user can save current configuration with **write memory** command. However, the dump file is not saved.

8 System Main Functions

8.1 VLAN

The first step in setting up your bridging network is to define VLAN on your switch. VLAN is a bridged network that is logically segmented by customer or function. Each VLAN contains group of ports called VLAN members. On the VLAN network, packets received on a port are forwarded only to ports that belong to the same VLAN as the receiving port. Network devices in different VLANs cannot communicate with one another without a Layer 3 switching device to route traffic between the VLANs. These VLANs improve performance because they reduce the propagation of local traffic, and they improve security benefits because they completely separate traffic.

Enlarged Network Bandwidth

Users belonged in each different VLAN can use more enlarged bandwidth than no VLAN composition because they do not receive unnecessary Broadcast information. A properly implemented VLAN will restrict multicast and unknown unicast traffic to only those links necessary to only those links necessary to reach members of the VLAN associated with that multicast (or unknown unicast) traffic.

Cost-Effective Way

When you use VLAN to prevent unnecessary traffic loading because of broadcast, you can get cost-effective network composition since switch is not needed.

Strengthened Security

When using a shared-bandwidth LAN, there is no inherent protection provided against unwanted eavesdropping. In addition to eavesdropping, a malicious user on a shared LAN can also induce problems by sending lots of traffic to specific targeted users or network as a whole. The only cure is to physically isolate the offending user. By creating logical partitions with VLAN technology, we further enhance the protections against both unwanted eavesdropping and spurious transmissions. As depicted in Figure, a properly implemented port-based VLAN allows free communication among the members of a given VLAN, but does not forward traffic among switch ports associated with members of different VLANs. That is, a VLAN configuration restricts traffic flow to a proper subnet comprising exactly those links connecting members of the VLAN. Users can eavesdrop only on the multicast and unknown unicast traffic within their own VLAN presumably the configured VLAN comprises a set of logically related users.

User Mobility

By defining a VLAN based on the addresses of the member stations, we can define a workgroup independent of the physical location of its members. Unicast and multicast traffic (including server advertisements) will propagate to all members of the VLAN so that they can communicate freely among themselves.

8.1.1 Port-Based VLAN

The simplest implicit mapping rule is known as port-based VLAN. A frame is assigned to a VLAN based solely on the switch port on which the frame arrives. In the example depicted in Figure, frames arriving on ports 1 through 4 are assigned to VLAN 1, frame from ports 5 through 8 are assigned to VLAN 2, and frames from ports 9 through 12 are assigned to VLAN 3.

Stations within a given VLAN can freely communicate among themselves using either unicast or multicast addressing. No communication is possible at the Data Link layer between stations connected to ports that are members of different VLANs. Communication among devices in separate VLANs can be accomplished at higher layers of the architecture, for example, by using a Network layer router with connections to two or more VLANs.

Multicast traffic, or traffic destined for an unknown unicast address arriving on any port, will be flooded only to those ports that are part of the same VLAN. This provides the desired traffic isolation and bandwidth preservation. The use of port-based VLANs effectively partitions a single switch into multiple sub-switches, one for each VLAN.

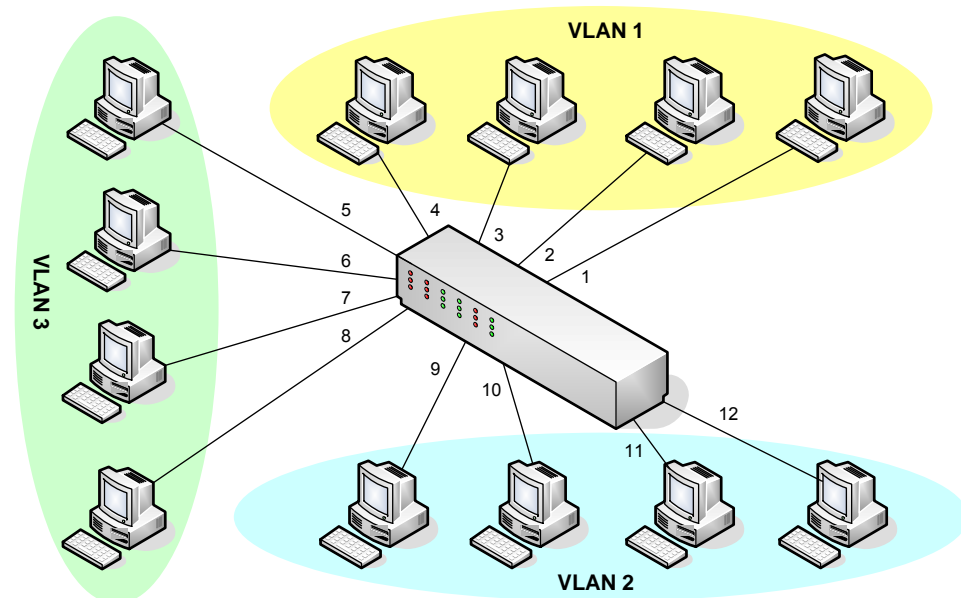


Fig. 8.1 Port-based VLAN

The IEEE 802.1q based ports on the switches support simultaneous tagged and untagged traffic. An 802.1q port is assigned a default port VLAN ID (PVID), and all untagged traffic is assumed to belong to the port default PVID. Thus, the ports participating in the VLANs accept packets bearing VLAN tags and transmit them to the port VLAN ID.

The below functions are explained.

- Creating VLAN
- Specifying PVID
- Assigning Port to VLAN
- Deleting VLAN
- Displaying VLAN

8.1.1.1 Creating VLAN

To configure VLAN on user's network, use the following command.

Command	Mode	Description
vlan create <i>VLANS</i>	Bridge	Creates new VLAN by assigning VLAN ID: VLANS: enter the number of VLAN ID (from 1 to 4094).



The variable VLANS is a particular set of bridged interfaces. Frames are bridged only among interfaces in the same VLAN.

8.1.1.2 Specifying PVID

By default, PVID 1 is specified to all ports. You can also configure PVID. To configure PVID in a port, use the following command.

Command	Mode	Description
vlan pvid <i>PORTS PVIDS</i>	Bridge	Configures VLAN PVID: PORTS: enter the port numbers. PVIDS: enter the PV IDs (1 to 4094 multiple entries possible).

8.1.1.3 Assigning Port to VLAN

To assign a port to VLAN, use the following command.

Command	Mode	Description
vlan add <i>VLANS PORTS {tagged untagged}</i>	Bridge	Assigns a port to VLAN: VLANS: enter the VLAN ID. PORTS: enter the port number.
vlan del <i>VLANS PORTS</i>		Deletes associated ports from specified VLAN: VLANS: enter the VLAN ID. PORTS: enter the port number to be deleted.



When you assign several ports to VLAN, you have to enter each port separated by a comma without space or use dash mark "-" to arrange port range.

8.1.1.4 Deleting VLAN

To delete VLAN, use the following command.

Command	Mode	Description
no vlan <i>VLANS</i>	Bridge	Deletes VLAN, enter the VLAN ID to be deleted.



When you delete VLAN, all ports must be removed from VLAN before, see the below procedure.

8.1.1.5 Displaying VLAN

To display a configuration of VLAN, use the following command.

Command	Mode	Description
show vlan [VLANs]	Enable Global Bridge	Shows the configuration for specific VLAN, enter VLAN ID.

8.1.2 Protocol-Based VLAN

User can use a VLAN mapping that associates a set of processes within stations to a VLAN rather than the stations themselves. Consider a network comprising devices supporting multiple protocol suites. Each device may have an IP protocol stack, an AppleTalk protocol stack, an IPX protocol stack and so on.

If we configure VLAN-aware switches such that they can associate a frame with a VLAN based on a combination of the station's MAC source address and the protocol stack in use, we can create separate VLANs for each set of protocol-specific applications.

To configure protocol-based VLAN, follow these steps.

1. Configure VLAN groups for the protocols you want to use.
2. Create a protocol group for each of the protocols you want to assign to a VLAN.
3. Then map the protocol for each interface to the appropriate VLAN

Command	Mode	Description
vlan pvid PORTS [ethertype ETHERTYPE] <1-4094>	Bridge	Configures protocol based VLAN. PORTS: input a port number ETHERTYPE: 0x800 1-4094: Vlan ID
no vlan pvid PORTS ethertype [ETHERTYPE]		Removes protocol based VLAN.

Because Protocol Based VLAN and normal VLAN run at the same time, Protocol Based VLAN operates only matched situation comparing below two cases.

1. When Untagged Frame comes in and matches with Protocol VLAN Table, tags PVID which configured on Protocol VLAN. But in no matched situation, tags PVID which configured on and operates VLAN.
2. When Tagged Frame comes in and VID is 0, it switches by Protocol VLAN Table. But if VID is not 0, it switches by normal VLAN Table.

8.1.3 Tagged VLAN

In a VLAN environment, a frame's association with a given VLAN is soft; the fact that a given frame exists on some physical cable does not imply its membership in any particular VLAN. VLAN association is determined by a set of rules applied to the frames by VLAN-aware stations and/or switches.

There are two methods for identifying the VLAN membership of a given frame:

- Parse the frame and apply the membership rules (implicit tagging).
- Provide an explicit VLAN identifier within the frame itself.

VLAN Tag

A VLAN tag is a predefined field in a frame that carries the VLAN identifier for that frame. VLAN tags are always applied by a VLAN –aware device. VLAN-tagging provides a number of benefits, but also carries some disadvantages.

Advantages	Disadvantages
VLAN association rules only need to be applied once.	Tags can only be interpreted by VLAN aware devices.
Only edge switches need to know the VLAN association rules.	Edge switches must strip tags before forwarding frames to legacy devices or VLAN-unaware domains.
Core switches can get higher performance by operating on an explicit VLAN identifier.	Insertion or removal of a tag requires recalculation of the FCS, possibly compromising frame integrity.
VLAN-aware end stations can further reduce the performance load of edge switches.	Tag insertion may increase the length of a frame beyond the maximum allowed by legacy equipment.

Tab. 8.1 Advantages and Disadvantages of Tagged VLAN

Mapping Frames to VLAN

From the perspective the VLAN-aware devices, the distinguishing characteristic of a VLAN is the means used to map a given frame to that VLAN. In the case of tagged frame, the mapping is simple – the tag contains the VLAN identifier for the frame, and the frame is assumed to belong to the indicated VLAN. That's all there is to it.

To configure the tagged VLAN, use the following command.

Command	Mode	Description
vlan add <i>VLANS PORTS tagged</i>	Bridge	Configures tagged VLAN on a port: VLANS: enter the VLAN ID. PORTS: enter the port number

8.1.4 VLAN Description

You can describe each VLAN with the following command

Command	Mode	Description
vlan description <i>VLANS DESC</i>	Bridge	Describes VLAN characteristic: VLANS: enter the VLAN ID. DESC: enter the detail description
no vlan description <i>VLANS</i>		Deletes the description about specified VLAN ID.

8.1.5 Displaying VLAN Information

User can display the VLAN information about Port based VLAN, Protocol based VLAN and QinQ.

Command	Mode	Description
show vlan	Enable Global Bridge	Shows all VLAN configurations.
show vlan VLANs		Shows a configuration for specific VLAN.
show vlan description		Shows a description for specific VLAN.
show vlan dot1q-tunnel		Shows QinQ configuration.
show vlan protocol		Shows VLAN based on protocol.

8.1.6 QinQ

QinQ or Double Tagging is one way for tunneling between networks

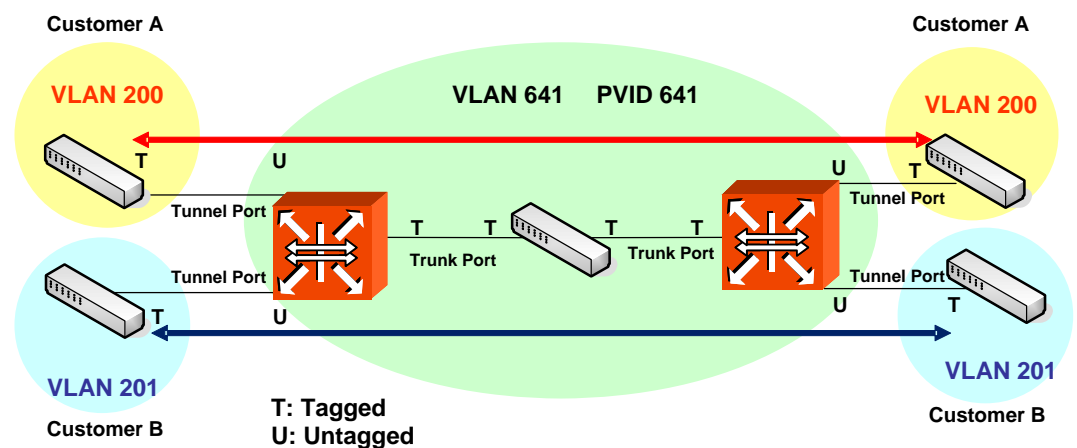
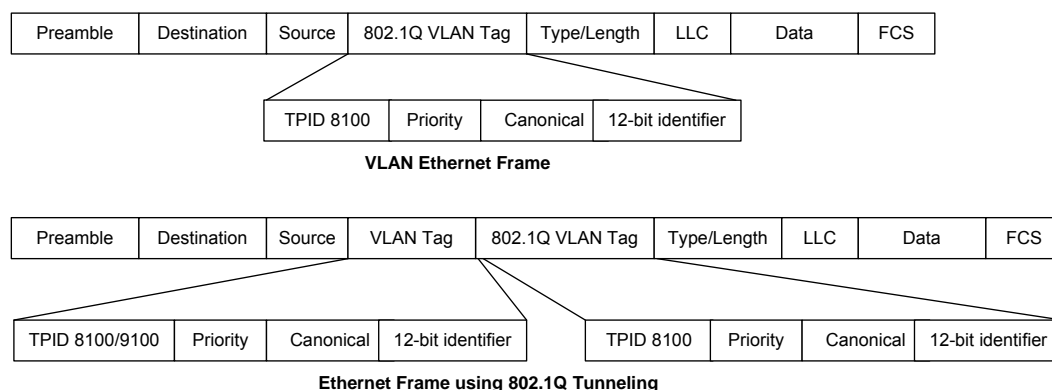


Fig. 8.2 Example of QinQ Configuration

If QinQ is configured on the hiD 6610 S311, it transmits packets adding another Tag to original Tag. Customer A group and customer B group can guarantee security because telecommunication is done between each VLANs at Double Tagging part.

Double tagging is implemented with another VLAN tag in Ethernet frame header.

**Fig. 8.3** QinQ Frame

Port which connected with Service Provider is Uplink port (internal), and which connected with customer is Access port (external).

Tunnel Port

By tunnel port we mean a LAN port that is configured to offer 802.1Q-tunneling support. A tunnel port is always connected to the end customer, and the input traffic to a tunnel port is always 802.1Q tagged traffic. The different customer VLANs existing in the traffic to a tunnel port shall be preserved when the traffic is carried across the network

Trunk Port

By trunk port we mean a LAN port that is configured to operate as an interswitch link/port, able of carrying double-tagged traffic. A trunk port is always connected to another trunk port on a different switch. Switching shall be performed between trunk ports and tunnels ports and between different trunk ports.

8.1.6.1 Double Tagging Operation

Step 1

If there is no SPVLAN Tag on received packet, SPVLAN Tag is added.

SPVLAN Tag = TPID : Configured TPID

VID : PVID of input port

Step 2

If received packet is tagged with CVLAN, the switch transmits it to uplink port changing to SPVLAN + CVLAN. When TPID value of received packet is same with TPID of port, it recognizes as SPVLAN, and if not as CVLAN.

Step 3

If Egress port is Access port (Access port is configured as Untagged), remove SPVLAN. If egress port is uplink port, transmit as it is.

Step 4

The hiD 6610 S311 switch has 0x8100 TPID value as default and other values are used as hexadecimal number.

8.1.6.2 Double Tagging Configuration

Step 1

Designate the QinQ port.

Command	Mode	Description
vlan dot1q-tunnel enable <i>PORTS</i>	Bridge	Configures a qinq port. PORTS: selects port number qinq to be enabled

Step 2

Configure the same PVID with the VLAN of peer network on the designated qinq port.

Command	Mode	Description
vlan pvid <i>PORTS</i> <1-4094>	Bridge	Configures a qinq port. PORTS: selects port number qinq to be enabled <1-4094>: VLAN ID

To disable double tagging, use the following command

Command	Mode	Description
vlan dot1q-tunnel disable <i>PORTS</i>	Bridge	Configures a qinq port. PORTS: a port qinq to be disabled



When you configure Double tagging on the hiD 6610 S311, consider the below attention list.

- DT and HTLS cannot be configured at the same time. (If switch should operate as DT, HTSL has to be disabled.)
- TPID value of all ports on switch is same.
- Access Port should be configured as Untagged, and Uplink port as Tagged.
- Ignore all tag information of port which comes from untagged port (Access Port).
- Port with DT function should be able to configure Jumbo function also

8.1.6.3 TPID Configuration

TPID (Tag Protocol Identifier) is a kind of Tag protocol, and it indicates the currently used tag information. User can change the TPID. By default the port which is configured as 802.1q (0x8100) cannot work as VLAN member.

Use the following command to set TPID on a QinQ port.

Command	Mode	Description
vlan dot1q-tunnel tpid <i>TPID</i>	Bridge	Configures TPID.

8.1.7 Layer 2 Isolation

Private VLAN is a kind of LAN Security function using by Cisco products, and it can be classified to Private VLAN and Private edge. Until now, there is no standard document of it.

Private VLAN Edge

Private VLAN edge (protected port) is a function in local switch. That is, it cannot work on between two different switches with protected ports. A protected port cannot transmit any traffic to other protected ports.

Private VLAN

Private VLAN provides L2 isolation within the same Broadcast Domain ports. That means another VLAN is created within a VLAN. There are three type of VLAN mode.

- **Promiscuous:** A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.
- **Isolated:** An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANS block all traffic to isolated ports except traffic from promiscuous ports. Traffic from isolated port is forwarded only promiscuous ports.
- **Community:** Community ports communicate among themselves and with their promiscuous ports. These interfaces separate at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

The difference between Private VLAN and Private VLAN edge is that PVLAN edge guarantees security for the ports in a VLAN using protected port and PVLAN guarantees port security by creating sub-VLAN with the three types (Promiscuous, Isolation, and Community). And because PVLAN edge can work on local switch, the isolation between two switches is impossible.

The hiD 6610 S311 provides Private VLAN function like Private VLAN edge of Cisco product. Because it does not create any sub-VLAN, port security is provided by port isolation. If you want to configure Private VLAN on the hiD 6610 S311 switch, refer to Port Isolation configuration.

8.1.7.1 Port Isolation

The Port Isolation feature is a method that restricts L2 switching between isolated ports in a VLAN. Nevertheless, flows between isolated port and non-isolated port are not restricted. If you use the **port protected** command, packet cannot be transmitted between protected ports. However, to non-protected ports, communication is possible.

To configure Port Isolation, use the following command.

Command	Mode	Description
port protected <i>PORTS</i>	Bridge	Enables port isolation.
no port protected [<i>PORTS</i>]		Disables port isolation.

8.1.7.2 Shared VLAN

This chapter is only for Layer 2 switch operation. The hiD 6610 S311 is Layer 3 switch, but it can be used for Layer 2 also. Because there is no routing information in Layer 2 switch, each VLAN cannot communicate. Especially, the uplink port should receive packets from all VLANs. Therefore, when you configure the hiD 6610 S311 as Layer 2 switch, the uplink ports have to be included in all VLANs.

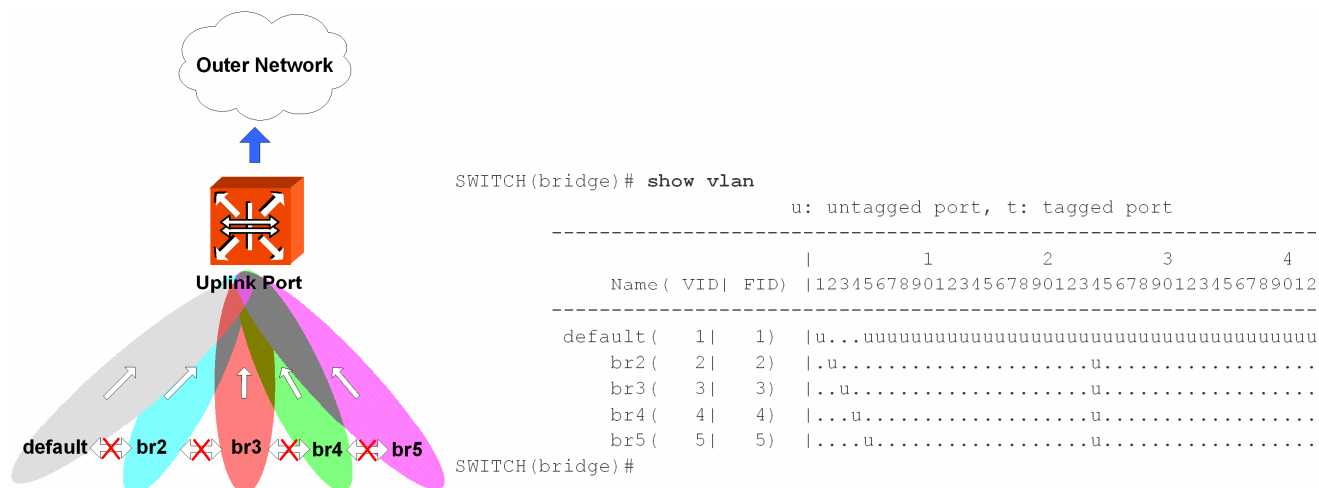


Fig. 8.4 In Case Packets Going Outside in Layer 2 environment

As above configuration with untagged packet, if an untagged packet comes into port 1, it is added with **tag 1** for PVID 1. And the uplink port 24 is also included in the default VLAN; it can transmit to port 24.

However, a problem is possible to occur for coming down untagged packets to uplink ports. If an untagged packet comes to uplink ports from outer network, the system does not know which PVID it has and where should it forward.

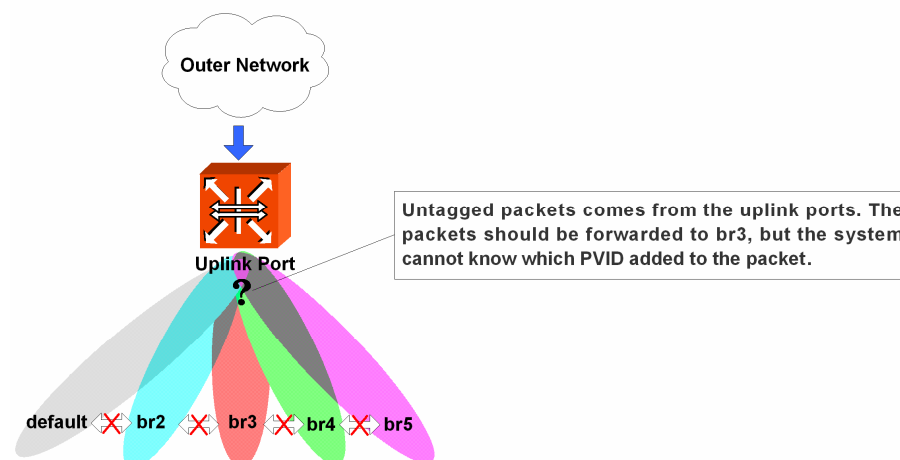


Fig. 8.5 In Case External Packets Enter under Layer 2 environment (1)

To transmit the untagged packet from uplink port to subscriber, a new VLAN should be created including all subscriber ports and uplink ports. This makes the uplink ports to recognize all other ports.

FID helps this packet forwarding. FDB is MAC Address Table that recorded in CPU. FDB table is made of FID (FDB Identification). Because the same FID is managed in the same MAC table, it can recognize how to process packet forwarding. If the FID is not same, the system cannot know the information from MAC table and floods the packets.

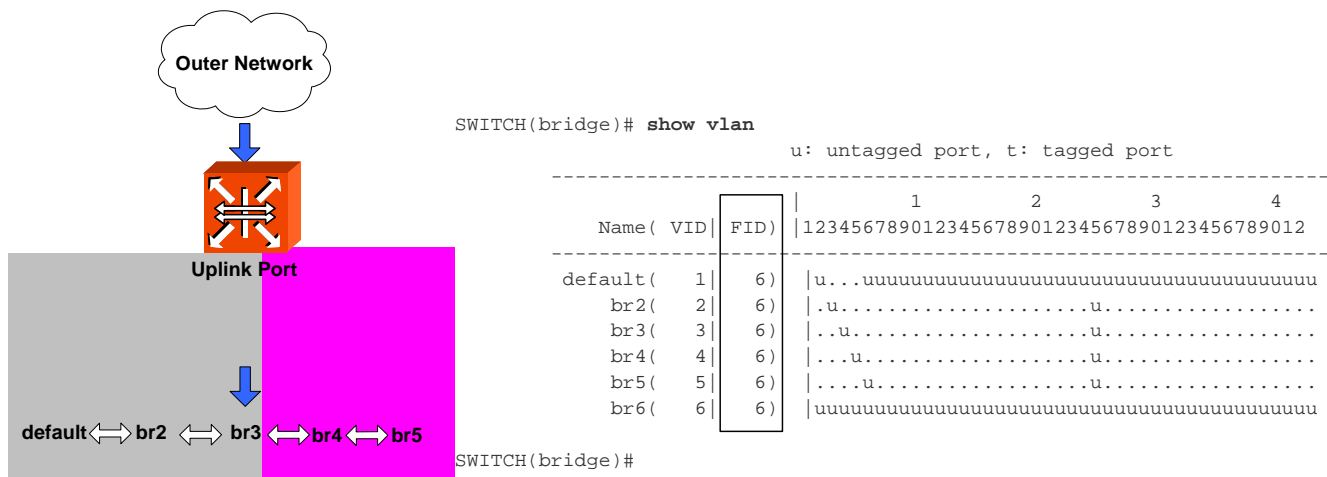


Fig. 8.6 In Case External Packets Enter under Layer 2 environment (2)

In conclusion, to use the hiD 6610 S311 as Layer 2 switch, user should add the uplink port to all VLANs and create new VLAN including all ports. If the communication between each VLAN is needed, FID should be same.

To configure FID, use the following command.

Command	Mode	Description
vlan fid <i>VLANS FID</i>	Bridge	Configures FID. VLANS: enters VLAN name FID: enters FID value

8.1.8 VLAN Translation

VLAN Translation is simply an action of Rule. This function is to translate the value of specific VLAN ID which classified by Rule. The switch makes Tag adding PVID on Untagged packets, and use Tagged Packet as it is. That is, all packets are tagged in the Switch, and VLAN Translation is to change the VLAN ID value of Tagged Packet in the Switch. This function is to adjust traffic flow by changing the VLAN ID of packet.

Step 1

Open *Rule Configuration* mode using **rule NAME create** command...

Step 2

Classify the packet that VLAN Translation will be applied by Rule..

Step 3

Designate the VLAN ID that will be changed in the first step by the **match vlan <1-4094>** command.

Step 4

Open *Bridge Configuration* mode using the **bridge** command.

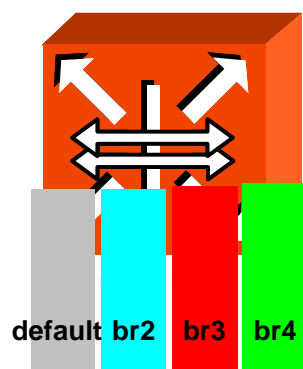
Step 5

Add the classified packet to VLAN members of the VLAN ID that will be changed.

8.1.9 Sample Configuration

[Sample Configuration 1] Configuring Port-based VLAN

The following is assigning vlan id of 2,3 and 4 to port 2, port 3, and port 4.



```
SWITCH(bridge)# vlan create 2
SWITCH(bridge)# vlan create 3
SWITCH(bridge)# vlan create 4
SWITCH(bridge)# vlan del default 2-4
SWITCH(bridge)# vlan add 2 2 untagged
SWITCH(bridge)# vlan add 3 3 untagged
SWITCH(bridge)# vlan add 4 4 untagged
SWITCH(bridge)# vlan pvid 2 2
SWITCH(bridge)# vlan pvid 3 3
SWITCH(bridge)# vlan pvid 4 4
SWITCH(bridge)# show vlan
```

u: untagged port, t: tagged port

[illegible]

port based VLAN.

[Sample Configuration 4] Configuring QinQ

10 port of SWITCH 1 and 11 port of SWITCH 2 are connected to the network where different VLANs are configured. To communicate without changing VLAN configuration of SWITCH 1 and SWITCH 2 which communicate with PVID 10, configure it as follows.



You should configure the ports connected to network communicating with PVID 11 as Tagged VLAN port.

< SWITCH 1 >

```
SWITCH(bridge)# vlan dot1q-tunnel enable 10
SWITCH(bridge)# vlan pvid 10 11
SWITCH(bridge)# show vlan dot1q-tunnel
Tag Protocol Id : 0x8100 (d: double-tagging port)
-----
|          1          2          3          4
Port | 123456789012345678901234567890123456789012
-----
dtag .....d.....
SWITCH(bridge)#
```

< SWITCH 2 >

```
SWITCH(bridge)# vlan dot1q-tunnel enable 11
SWITCH(bridge)# vlan pvid 11 11
SWITCH(bridge)# show vlan dot1q-tunnel
Tag Protocol Id : 0x8100 (d: double-tagging port)
-----
|          1          2          3          4
Port | 123456789012345678901234567890123456789012
-----
dtag .....d.....
SWITCH(bridge)#
```


8.2 Link Aggregation

Link Aggregation Control Protocol (LACP) complying with IEEE 802.3ad bundles several physical ports together to one logical port so that user can get enlarged bandwidth.

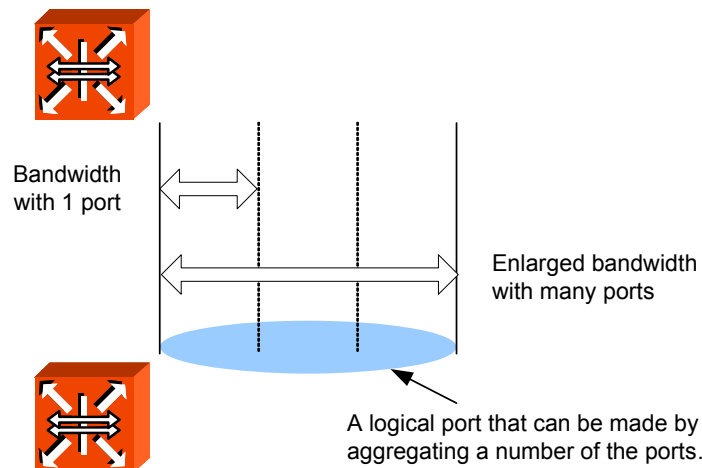


Fig. 8.7 Link Aggregation

The hiD 6610 S311 supports two kinds of link aggregation as port trunk and LACP. There's a little difference in these two ways. In case of port trucking, it is quite troublesome to set the configuration manually and the rate to adjust to the network environment changes when connecting to the switch using logical port. However, if the user configures physical port aggregated with the logical port in each switches, the switches are connected as the configuration. Therefore it is easier for user to configure comparing to the port trunk and could quickly respond to the environmental changes.

8.2.1 Port Trunk

Port trucking enables you to dynamically group similarly configured interfaces into a single logical link (aggregated port) to increase bandwidth, while reducing the traffic congestion.

8.2.1.1 Configuring Port Trunk

To make logical port by aggregating the ports, use the following command.

Command	Mode	Description
trunk add <0-13> <i>PORTS</i> { <i>dstip</i> <i>dstmac</i> <i>srcdstip</i> <i>srcdstmac</i> <i>srcip</i> <i>srcmac</i> }	Bridge	Adds a port to the aggregation group and designates physical port as logical port and decide which packets are transmitted to the aggregated port. 1-13: Trunk Group ID



It is possible to input trunk group-ID from 0 to 13 because the hiD 6610 S311 supports 14 logical aggregated ports, and group-ID of port trunk and Aggregator-number of LACP cannot be repeatedly configured.



For the hiD 6610 S311, source destination MAC address is basically used to decide packet route.

If packets enter to logical port aggregating several ports and there's no way to decide packet route, the packets could be gathered on particular member port so that it is not possible to use logical port effectively. Therefore hiD 6610 S311 is configured to decide the way of packet route in order to divide on member port effectively when packets enter. It is decided with Source IP address, Destination IP address, Source MAC address, Destination Mac address and the user could get information of packets to decided packet route.

- **dstip**: Destination IP address
- **dstmac**: Destination MAC address
- **srcdstip**: Refer to both Source IP address and Destination IP address
- **srcdstmac**: Refer to both Source MAC address and Destination MAC address
- **srcip**: Source IP address
- **srcmac**: Source MAC address.

The port designated as member port of port trunk is automatically deleted from existing VLAN. Therefore, if member port and aggregated port exist in other VLAN, VLAN configuration should be changed for the aggregated port.

8.2.1.2 Disabling Port Trunk

To remove the configured port trunk from specified trunk group, use the following command.

Command	Mode	Description
trunk del <0-13> <i>PORTS</i>	Bridge	Releases a configured trunk port.



If the user deleted member port from logical port or release port trunk, they are automatically contained as default VLAN.

8.2.1.3 Displaying Port Trunk Configuration

To display a configuration of port trunk, use the following command.

Command	Mode	Description
show trunk	Enable Global Bridge	Shows a configuration for trunk.

8.2.2 Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (LACP) is the function of using wider bandwidth by aggregating more than two ports as a logical port as previously stated port trunk function. If the integrated port by configuring from port trunk is in other VLAN which is different from VLAN where existing member port is originally belong to, it should be moved to VLAN where the existing member port is belong to. However, the integrated port configured by LACP is automatically added to appropriate VLAN.



The LACP aggregator from LACP could support up to 14 so that it is possible to input aggregator number from 0 to 13, and group ID of port trunk and aggregator number of LACP cannot be configured repeatedly.

The following explains how to configure LACP.

- Configuring LACP
- Packet Route
- Operating Mode of Member Port
- Priority of Switch
- Identifying Member Ports within LACP
- BPDU Transmission Rate
- Key value of Member Port
- Priority
- Displaying LACP Configuration

8.2.2.1 Configuring LACP

Step 1

Activate LACP function, using the following command.

Command	Mode	Description
lacp aggregator <i>AGGREGATIONS</i>	Bridge	Enables LACP of designated Aggregator-number: AGGREGATIONS: select aggregator ID that should be enabled for LACP (valid value from 0 to 13).
no lacp aggregator <i>AGGREGATIONS</i>		Disables LACP for designated Aggregator-number, select the aggregator ID that should be disabled for LACP.

Step 2

Configure the physical port that is a member of aggregated port. In order to configure the member port, use the following command.

Command	Mode	Description
lacp port <i>PORTS</i>	Bridge	Configures physical port that is member port of aggregator; select the port number(s) that should be enabled for LACP.
no lacp port <i>PORTS</i>		Deletes member port of Aggregator, select the port number(s) that should be disabled for LACP.

8.2.2.2 Packet Route

When packets enter to logical port integrating several ports, if there's no process to decide the packet route, it is not possible to use logical port effectively from focusing packets on a particular member port.

If these packets enter to logical port aggregating several ports and there's no way to decide packet route, the packets could be gathered on particular member port so that it is not possible to use logical port effectively.

Therefore the hiD 6610 S311 is configured to decide the way of packet route in order to divide on member port effectively when packets are transmitted. It can be selected with Source IP address, destination IP address, source MAC address, destination MAC address and the user could get the information of packets to decided packet route.

- **dstip**: Destination IP address
- **dstmac**: Destination MAC address
- **srcdstip**: Runs by reference to both Source IP address and Destination IP address
- **srcdstmac**: Source MAC address and Destination MAC address
- **srcip**: Source IP address
- **srcmac**: Source MAC address.



For the hiD 6610 S311, **srcdstmac** (source MAC address and destination MAC address) is basically used to decide packet route.

After configuring aggregator, you should configure packets transmitting aggregator port. The following is the command of configuring packets transmitting aggregator port.

Command	Mode	Description
lacp aggregator distmode AGGREGATIONS {srcmac dstmac srcdstmac srcip dstip srcdstip}	Bridge	Defines packets transmitted by way of aggregator which is a logical aggregated port: AGGREGATIONS: select the aggregator ID <0-13>.

To disable configuring packets, use the following command.

Command	Mode	Description
no lacp aggregator AGGREGATIONS	Bridge	Deletes destination MAC address, select the aggregator ID.

8.2.2.3 Operating Mode of Member Port

After configuring member port, configure the mode of member port. There are two kinds of mode *Active* mode and *Passive* mode in member port. The port of *Passive* mode starts LACP when there's *Active* mode on the port of opposite switch. The priority of *Active* mode is higher than that of *Passive* mode so that the port of *Passive* mode follows the port of *Active* mode.



If each member port of the connected switch is configured as *Active* mode and *Passive* mode, *Active* mode is the standard. If both switches are configured as *Passive* mode, link for member ports of two switches is not realized.

To configure the mode of member port, use the following command.

Command	Mode	Description
lacp port activity <i>PORTS</i> { active passive }	Bridge	Configure the mode of member port, select the member port number. (default: active)

To delete an operating mode of configured member port, use the following command.

Command	Mode	Description
no lacp port activity <i>PORTS</i>	Bridge	Deletes operation mode of configured member port, select the member port number.

8.2.2.4 Identifying Member Ports within LACP

The port configured as member port is basically configured to aggregate to LACP. However, even though the configuration as member port is not released, they could operate as independent port without being aggregated to LACP. These independent ports cannot be configured as trunk port because they are independent from being aggregated to LACP under the condition of being configured as member port.

To configure member port to aggregate to LACP, use the following command.

Command	Mode	Description
lacp port aggregation <i>PORTS</i> { aggregatable individual }	Bridge	Designates whether a member port joins LACP or not, select the member port should be included. (default: aggregatable)

To clear aggregated to LACP of configured member port, use the following command.

Command	Mode	Description
no lacp port aggregation <i>PORTS</i>	Bridge	Deletes the configured member port in LACP, select the member port.

8.2.2.5 BPDU Transmission Rate

Member port transmits BPDU with its information. For the hiD 6610 S311, it is possible to configure the BPDU transmission rate, use the following command.

Command	Mode	Description
lacp port timeout <i>PORTS</i> { short long }	Bridge	Configures BPDU transmission rate: PORTS: select the port number. short: fast rate (once every 1 sec) long: slow rate (30 sec: default)

To clear BPDU transmission rate, use the following command (clear means long timeout).

Command	Mode	Description
no lacp port timeout <i>PORTS</i>	Bridge	Deletes BPDU transmission rate of configured member port, select the port number.

8.2.2.6 Key value of Member Port

Member port of LACP has key value. All member ports in one aggregator have same key values. To make an aggregator consisted of specified member ports, configure different key value with key value of another port.

Command	Mode	Description
lacp port admin-key <i>PORTS</i> <1-15>	Bridge	Configures key value of member port: PORTS: select the port number. 1-15: select the port key value. (default: 1)

To delete key value of configured member port, use the following command.

Command	Mode	Description
no lacp port admin-key <i>PORTS</i>	Bridge	Deletes key value of selected member port, select the member port number.

8.2.2.7 Priority of Member Port

To configure priority of LACP member port, use the following command.

Command	Mode	Description
lacp port priority <i>PORTS</i> <1-65535>	Bridge	Sets the LACP priority of member port, select the port number. (default: 32768)

To remove port priority of configured member port, use the following command.

Command	Mode	Description
no lacp port priority <i>PORTS</i>	Bridge	Deletes port priority of selected member port, select the member port number.

8.2.2.8 Priority of Switch

In case the member ports of connected switches are configured as Active mode (LACP system enabled), it is required to configure which switch would be a standard for it. For this case, the user could configure the priority on switch. The following is the command of configuring the priority of the switch in LACP function.

Command	Mode	Description
lacp system priority <1-65535>	Bridge	Sets the priority of the switch in LACP function, enter the switch system priority. (default: 32768)

To delete the priority of configured switch, use the following command.

Command	Mode	Description
no lacp system priority	Bridge	Clears the priority of the configured switch.

8.2.2.9 Displaying LACP Configuration

To display a configured LACP, use the following command.

Command	Mode	Description
show lacp aggregator	Enable Global Bridge	Shows the information of aggregated port.
show lacp aggregator <i>AGGREGATIONS</i>		Shows the information of selected aggregated port.
show lacp port		Shows the information of member port.
show lacp port <i>PORTS</i>		Shows the information of appropriated member port.
show lacp statistics		Shows aggregator statistics.

To clear LACP statistics information, use the following command.

Command	Mode	Description
clear lacp statistics	Enable Global Bridge	Clears the information of statistics.

8.3 Spanning-Tree Protocol (STP)

LAN, which is composed of double-path like token ring, has the advantage that it is possible to access in case of disconnection with one path. However, there is another problem named Loop when you always use the double-path.

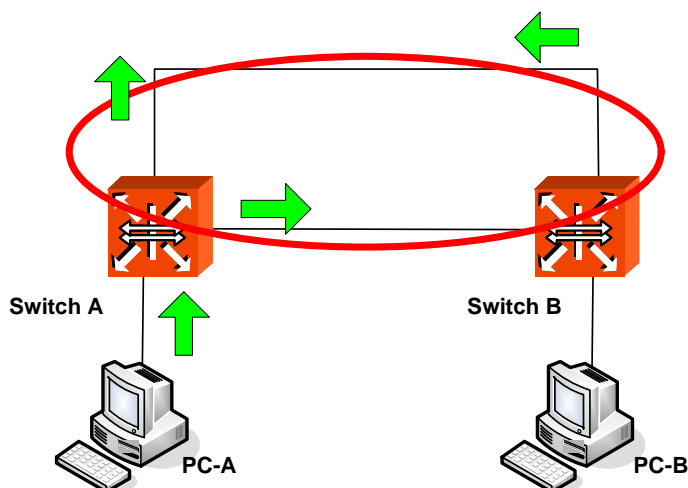


Fig. 8.8 Example of Loop

Loop is when there are more than one path between switches (SWITCH A, B), PC A sends packet through broadcast or multicast and then the packet keeps rotating. It causes superfluous data-transmission and network fault.

STP (Spanning-Tree Protocol) is the function to prevent Loop in LAN with more than two paths and to utilize the double-path efficiently. It specifies in IEEE 802.1d. If STP is configured, there is no Loop since it chooses more effective path of them and closes the other path. In other words, when SWITCH C in the below figure sends packet to SWITCH B, path 1 is chosen and path 2 is blocked.

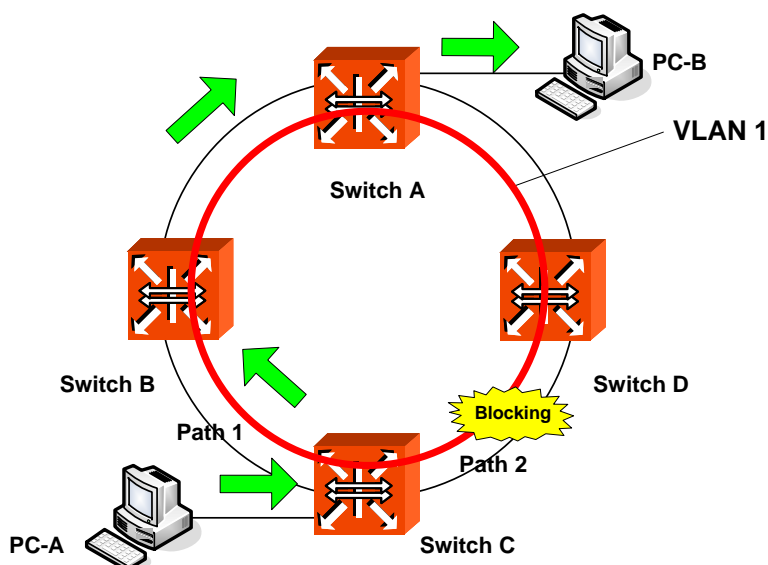


Fig. 8.9 Principle of Spanning Tree Protocol

Meanwhile, RSTP (Rapid Spanning-Tree Protocol) defined in IEEE 802.1w innovate reduces the time of network convergence on STP (Spanning-Tree Protocol). It is easy and fast to configure new protocol.

Also, 802.1w includes 802.1d inside, so it can provide compatibility with 802.1d. For more detail description of STP and RSTP, refer to the following.

- STP Operation
- RSTP Operation
- MSTP Operation
- Configuring STP/RSTP/MSTP/PVSTP/PVRSTP Mode (Required)
- Configuring STP/RSTP/MSTP
- Configuring PVSTP/PVRSTP
- Root Guard
- Restarting Protocol Migration
- Bridge Protocol Data Unit Configuration
- Sample Configuration

8.3.1 STP Operation

The 802.1d STP defines port state as blocking, listening, learning, and forwarding. When STP is configured in LAN with double-path, switches exchange their information including bridge ID. It is named as BPDU (Bridge Protocol Data Unit). Switches decide port state based on the exchanged BPDU and automatically decide optimized path to communicate with the root switch.

Root Switch

The most important information to decide the root switch is bridge ID. Bridge ID is composed of 2 bytes-priority and 6 bytes-MAC address. The root switch is decided with the lowest bridge ID.

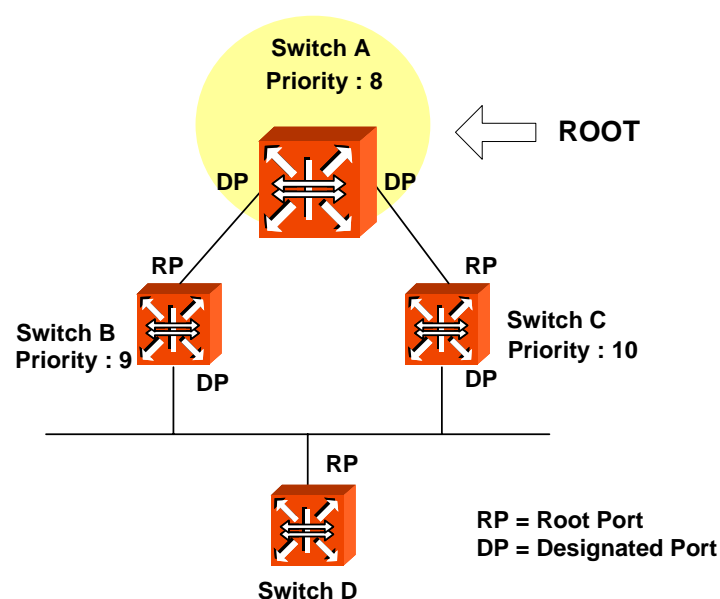


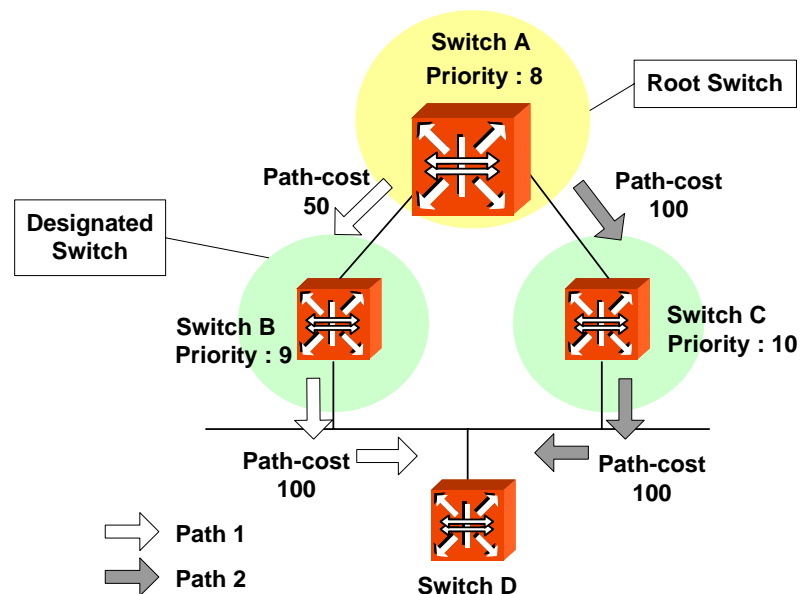
Fig. 8.10 Root Switch

After configuring STP, these switches exchange their information. The priority of SWITCH A is 8, the priority of SWITCH B is 9 and the priority of SWITCH C is 10. In this case, SWITCH A is automatically configured as a root switch.

Designated Switch

After deciding a root switch, while SWITCH A transmits packets to SWITCH C, SWITCH A compares exchanged BPDU to decide the path. The most important information to decide path is the path-cost. Path-cost depends on transmission rate of LAN interface and path with lower path-cost is selected.

The standard to decide designated switch is total root path-cost which is added with path-cost to root. Path-cost depends on transmit rate of switch LAN interface and switch with lower path-cost is selected to be designated switch.



(PATH 1 = 50 + 100 = 150, PATH 2 = 100 + 100 = 200, PATH 1 < PATH 2, ∴ **PATH 1 selected**)

Fig. 8.11 Designated Switch

In case of the above picture showing SWITCH C sends packet, path-cost of PATH 1 is 150 and path-cost of PATH 2 is total 200 (100 + 100; path-cost of SWITCH C to B + path-cost of SWITCH B to C). Therefore lower path-cost, PATH 1 is chosen. In this case, port connected to Root switch is named Root port. In the above picture, port of SWITCH C connected to SWITCH A as Root switch is Root port. There can be only one Root port on equipment.

The standard to decide designated switch is total root path-cost which is added with path-cost to root. Switch with lower path-cost is selected to be designated switch. When root path-costs are same, bridge ID is compared.

Designated Port and Root Port

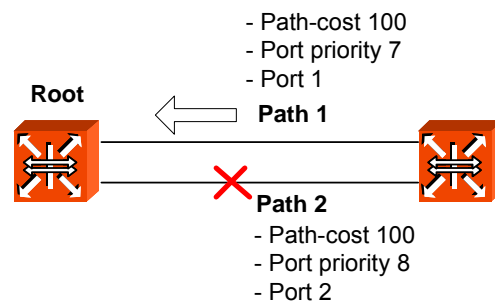
A Root Port is the port in the active topology that provides connectivity from the Designated Switch toward the root. A Designated Port is a port in the active topology used to forward traffic away from the root onto the link for which this switch is the Designated Switch. That is; except root port in each switch, selected port to communicate is designated port.

Port Priority

Meanwhile, when path-costs of two paths are same, port-priority is compared. As the below picture, suppose that two switches are connected. Since the path-costs of two paths are 100, same, their port priorities are compared and port with smaller port priority is selected to transmit packet.



All these functions are automatically performed by BPDU, which is the information of switch. It is also possible to configure BPDU to modify root switch or path manually.



(path-cost of PATH 1 = path-cost of PATH 2 = 100 \therefore unable to compare
PATH 1 port priority = 7, PATH 2 port priority = 8, PATH 1 < PATH 2, \therefore **PATH 1 is chosen**)

Fig. 8.12 Port Priority

Port States

Each port on a switch can be in one of five states.

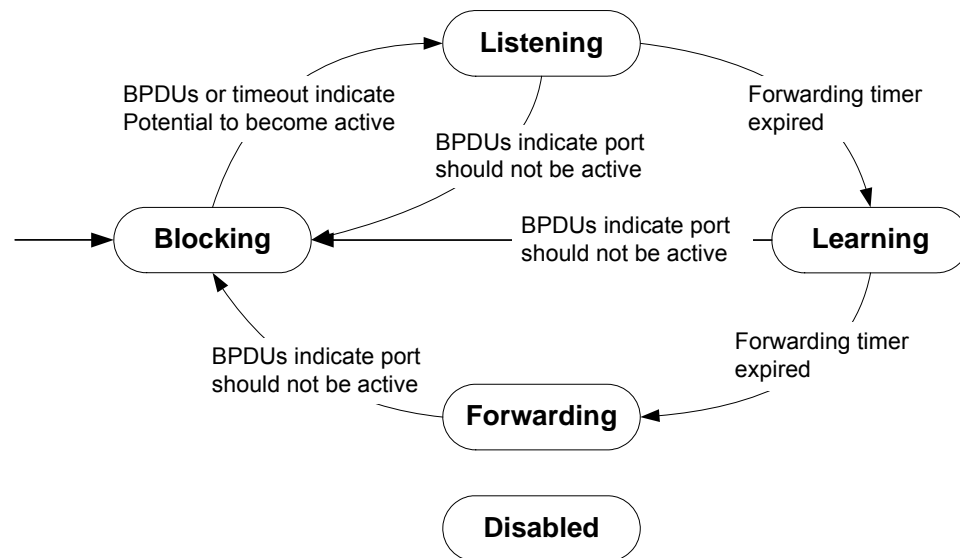


Fig. 8.13 Port State

- Blocking**
 a port that is enabled, but that is neither a Designated port nor a Root port, will be in the blocking state. A blocking port will not receive or forward data frames, nor will it transmit BPDUs, but instead it will listen for other's BPDUs to determine if and when the port should consider becoming active in the spanning tree.
- Listening**
 the port is still not forwarding data traffic, but is listening to BPDUs in order to compute the spanning tree. The port is comparing its own information (path cost, Bridge Identifier, Port Identifier) with information received from other candidates and deciding which is best suited for inclusion in the spanning tree.
- Learning**
 the port is preparing to forward data traffic. The port waits for a period of time to build its MAC address table before actually forwarding data traffic. This time is the forwarding delay.
- Forwarding**
 After some time learning address, it is allowed to forward data frame. This is the steady state for a switch port in the active spanning tree.
- Disabled**
 When disabled, a port will neither receive nor transmit data or BPDUs. A port is in this state because it is broken or disabled by administrator.

8.3.2 RSTP Operation

STP or RSTP is configured on network where Loop can be created. However, RSTP is more rapidly progressed than STP at the stage of reaching to the last topology. This section describes how the RSTP more improved than STP works. It contains the below sections.

- Port States
- BPDU Policy
- Rapid Network Convergence
- Compatibility with 802.1d.

Port States

RSTP defines port states as discarding, learning, and forwarding. Blocking of 802.1d and listening is combined into discarding. Same as STP, root port and designated port are decided by port state. But a port in blocking state is divided into alternate port and backup port. Alternate port means a port blocking BPDUs of priority of high numerical value from other switches, and backup port means a port blocking BPDUs of priority of high numerical value from another port of same equipment.

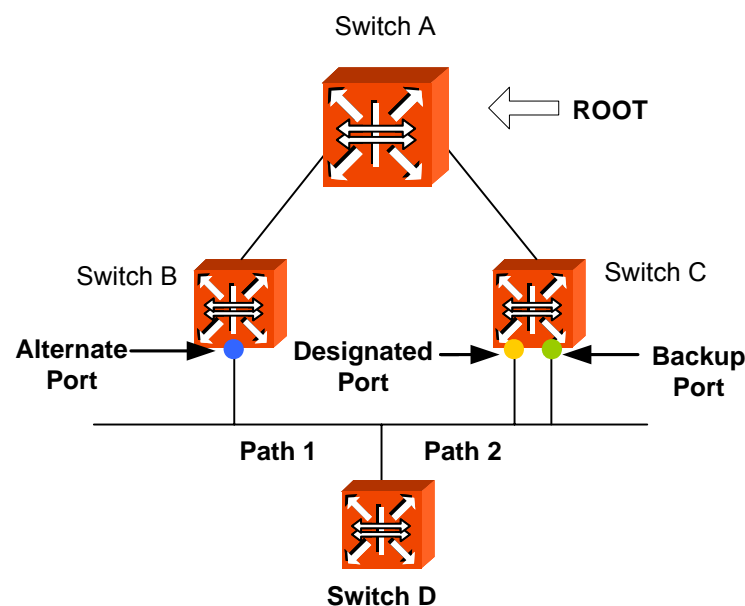


Fig. 8.14 Alternate Port and Backup port

The difference of between alternate port and backup port is that alternate port can alternate path of packet when there is a problem between Root switch and SWITCH C but Backup port cannot provide stable connection in that case.

BPDU Policy

802.1d forwards BPDU following Hello-time installed in root switch and the other switch except root switch its own BPDU only when receiving BPDU from root switch. However, in 802.1w not only root switch but also all the other switches forward BPDU following Hello-time. BPDU is more frequently changed than the interval root switch exchanges, but with 802.1w it becomes faster to be master of the situation of changing network.

By the way, when low BPDU is received from root switch or designated switch, it is immediately accepted. For example, suppose that root switch is disconnected to SWITCH B. Then, SWITCH B is considered to be root because of the disconnection and forwards BPDU.

However, SWITCH C recognizes root existing, so it transmits BPDU including information of root to Bridge B. Thus, SWITCH B configures a port connected to SWITCH C as new root port.

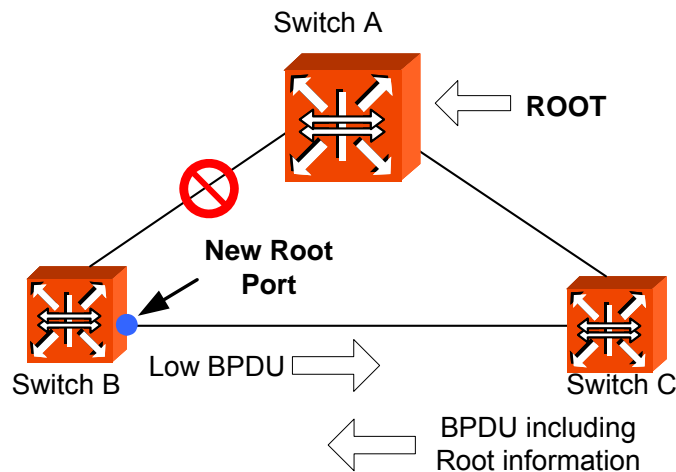


Fig. 8.15 Example of Receiving Low BPDU

Rapid Network Convergence

A new link is connected between SWITCH A and root. Root and SWITCH A is not directly connected, but indirectly through SWITCH D. After SWITCH A is newly connected to root, packet cannot be transmitted between the ports because state of two switches becomes listening, and no loop is created.

In this state, if root transmits BPDU to SWITCH A, SWITCH A transmits new BPDU to SWITCH A and SWITCH C, switch C transmits new BPDU to SWITCH D. SWITCH D, which received BPDU from SWITCH C makes port connected to SWITCH C Blocking state to prevent loop after new link.

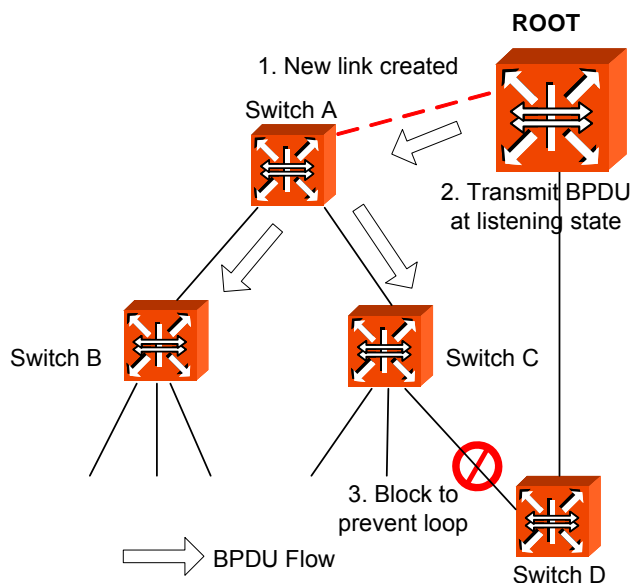


Fig. 8.16 Convergence of 802.1d Network

This is very an epochal way of preventing a loop. The matter is that communication is disconnected during two times of BPDU Forward-delay till a port connected to switch D and SWITCH C is blocked. Then, right after the connection, it is possible to transmit BPDU although packet cannot be transmitted between switch A and root.

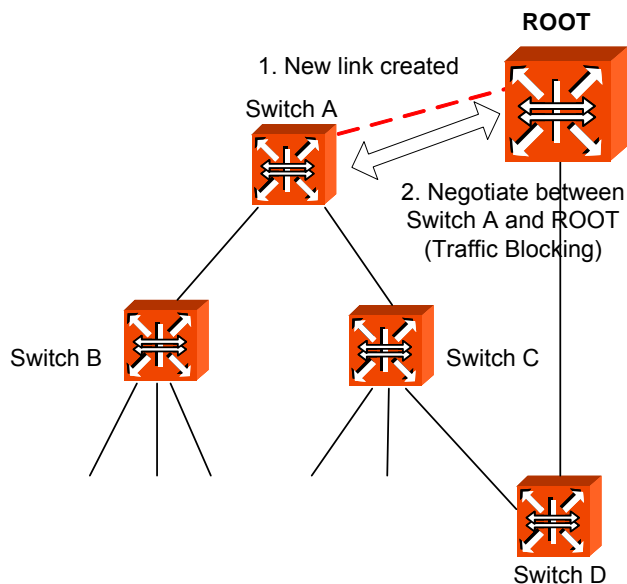


Fig. 8.17 Network Convergence of 802.1w (1)

SWITCH A negotiates with root through BPDUs. To make link between SWITCH A and root, port state of non-edge designated port of SWITCH is changed to blocking. Although SWITCH A is connected to root, loop will not be created because SWITCH A is blocked to SWITCH B and C. In this state, BPDUs from root are transmitted to SWITCH B and C through SWITCH A. To configure forwarding state of SWITCH A, SWITCH A negotiates with SWITCH B and SWITCH C.

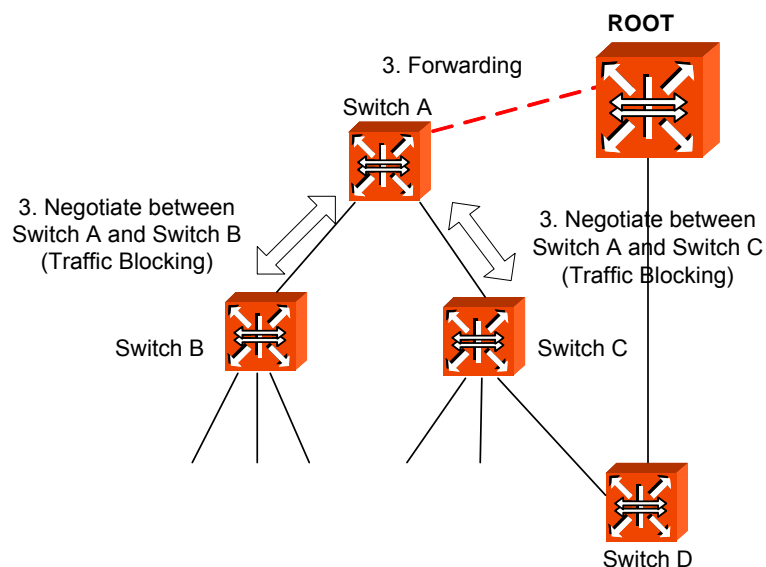


Fig. 8.18 Network Convergence of 802.1w (2)

SWITCH B has only edge-designated port. Edge designated does not cause loop, so it is defined in 802.1w to be changed to forwarding state. Therefore, SWITCH B does not need to block specific port to forwarding state of SWITCH A. However since SWITCH C has a port connected to SWITCH D, you should make blocking state of the port.

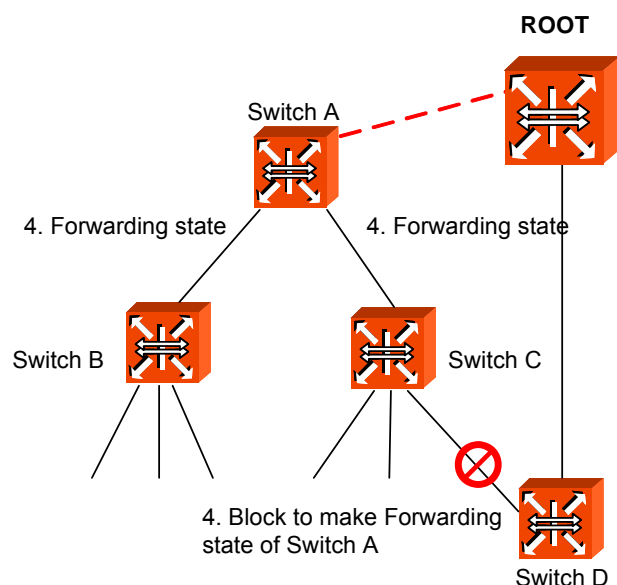


Fig. 8.19 Network Convergence of 802.1w (3)

It is same with 802.1d to block the connection of SWITCH D and SWITCH C. However, 802.1w does not need any configured time to negotiate between switches to make forwarding state of specific port. So it is very fast progressed. During progress to forwarding state of port, listening and learning are not needed. These negotiations use BPDU.

Compatibility with 802.1d

RSTP internally includes STP, so it has compatibility with 802.1d. Therefore, RSTP can recognize BPDU of STP. But, STP cannot recognize BPDU of RSTP. For example, assume that SWITCH A and SWITCH B are operated as RSTP and SWITCH A is connected to SWITCH C as designated switch. Since SWITCH C, which is 802.1d ignores RSTP BPDU, it is interpreted that switch C is not connected to any switch or segment.

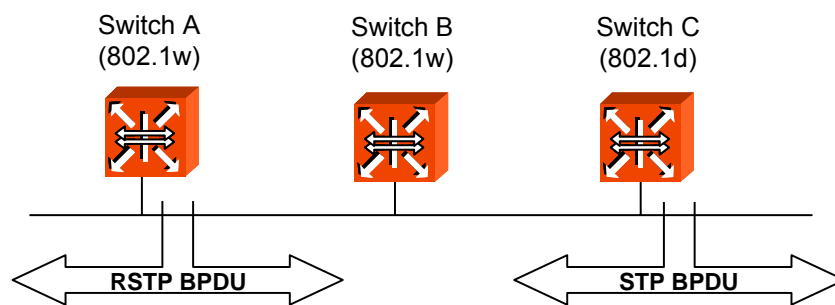


Fig. 8.20 Compatibility with 802.1d (1)

However, SWITCH A converts a port received BPDU into RSTP of 802.1d because it can read BPDU of SWITCH C. Then SWITCH C can read BPDU of SWITCH A and accepts SWITCH A as designated switch.

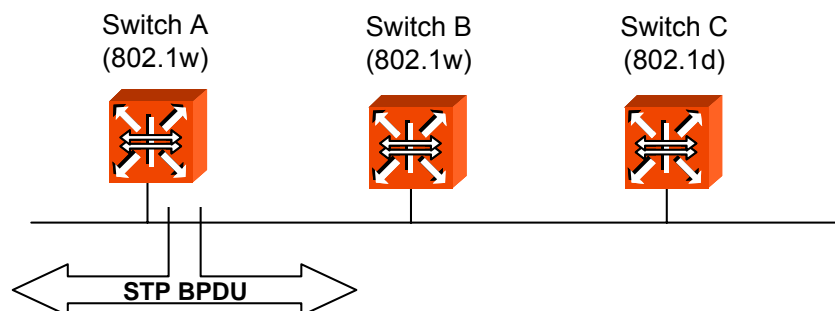


Fig. 8.21 Compatibility with 802.1d (2)

8.3.3 MSTP Operation

To operate the network more effectively, the hiD 6610 S311 uses MSTP (Multiple Spanning-Tree Protocol). It constitutes the network with VLAN subdividing existing LAN domain logically and configure the route by VLAN or VLAN group instead of existing routing protocol.

Operation

Here explains how STP/MSTP differently operates on the LAN. Suppose to configure 100 of VLAN from Switch A to B, C. In case of STP, there's only a STP on all of VLAN and it does not provide multiple instances.

While existing STP is a protocol to prevent Loop in a LAN domain establishes STP per VLAN in order to realize routing suitable to VLAN environment.

It does not need to calculate all STP for several VLAN so that traffic overload could be reduced. By reducing unnecessary overload and providing multiple transmission route for data forwarding, it realizes load balancing and provides many VLAN through Instances.

MSTP

In MSTP, VLAN is classified to groups with same Configuration ID. Configuration ID is composed of Revision name, Region name and VLAN/Instance mapping. Therefore, to have same configuration ID, all of these tree conditions should be the same. VLAN classified with same configuration ID is called MST region. In a region, there's only a STP so that it is possible to reduce the number of STP comparing to PVSTP. There's no limitation for region in a network environment but it is possible to generate Instances up to 64. Therefore instances can be generated from 1 to 64. Spanning-tree which operates in each region is IST (Internal Spanning-Tree). CST is applied by connecting each spanning-tree of region. Instance 0 means that there is not any Instance generated from grouping VLAN, that is, it does not operate as MSTP. Therefore Instance 0 exists on all the ports of the equipment. After starting MSTP, all the switches in CST exchanges BPDU and CST Root is decided by comparing their BPDU. Here, the switches that don't operate with MSTP have instance 0 so that they can also join BPDU exchanges. The operation of deciding CST Root is CIST (Common & Internal Spanning-Tree).

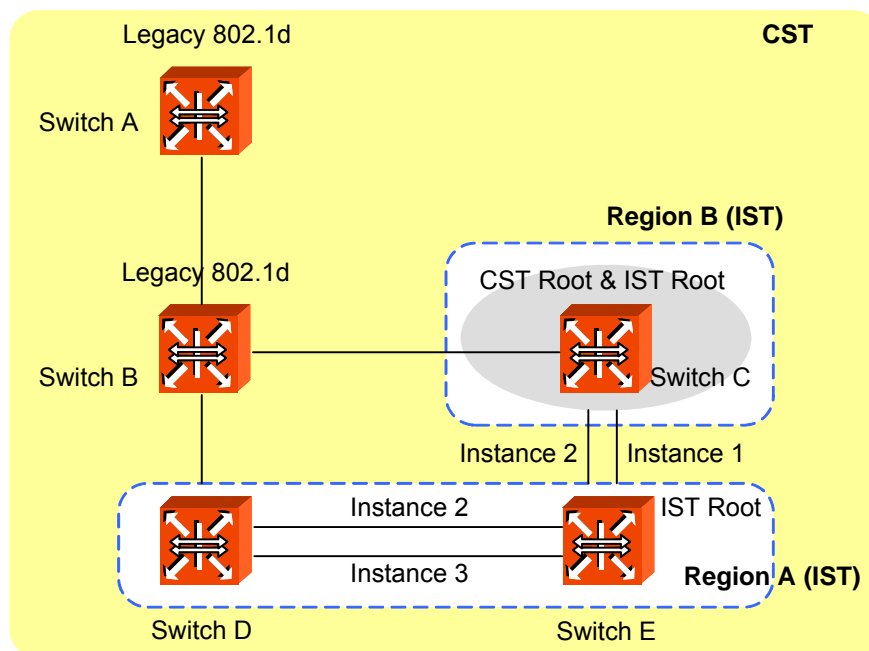


Fig. 8.22 CST and IST of MSTP (1)

In CST, A and B are the switches operating with STP and C, D and, E are those operating with MSTP. First, in CST, CIST is established to decide CST Root. After CST root is decided, the closest switch to CST root is decided as IST root of the region. Here, CST root in IST is IST root.

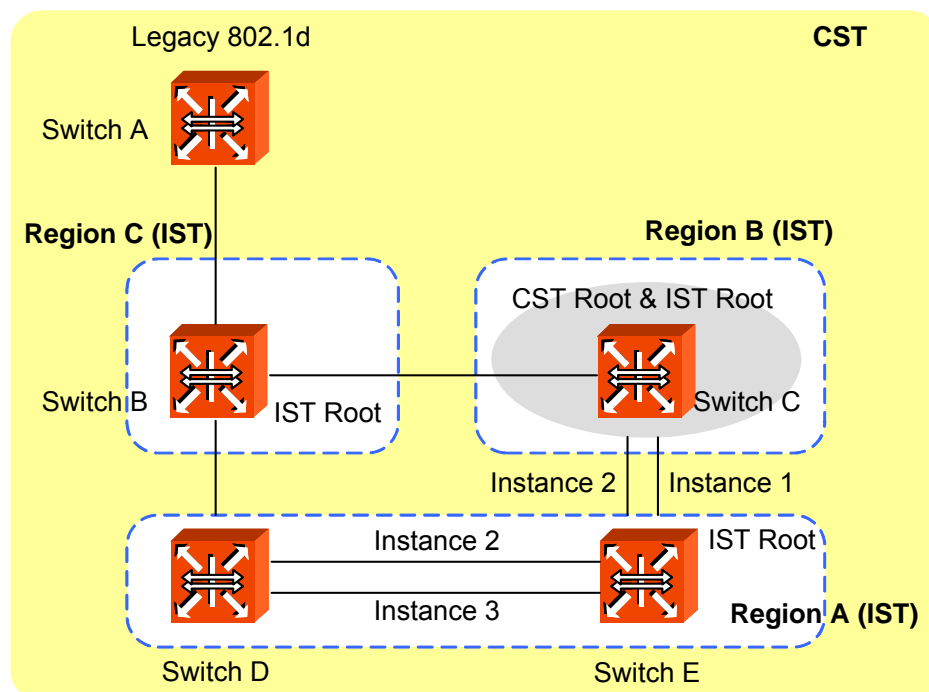


Fig. 8.23 CST and IST of MSTP (2)

In above situation, if B operates with MSTP, B will send its BPDU to CST root and IST root in order to request itself to be CST root. However, if any BPDU having higher priority than that of B is sent, B cannot be CST root.

For the hiD 6610 S311, the commands configuring MSTP are also used to configure STP and RSTP.

8.3.4 Configuring STP/RSTP/MSTP/PVSTP/PVRSTP Mode (Required)

First of all, you need to configure force-version to decide the mode before STP is configured. To decide force-version of the switch, use the following command.

Command	Mode	Description
stp force-version {stp rstp mstp pvstp pvrstp}	Bridge	Configures Force-version in the bridge.

To delete STP configuration from the switch, use the following command.

Command	Mode	Description
no stp force-version	Bridge	Removes force-version configuration.

8.3.5 Configuring STP/RSTP/MSTP

To configure STP and RSTP, use the following steps.

Step 1

Decide STP mode using the **stp force-version {stp | rstp}** command.

Step 2

Activate MST daemon using the **stp mst enable** command.

Step 3

Configure detail options if specific commands are required.

8.3.5.1 Activating STP/RSTP/MSTP

To enable/disable STP, RSTP, and MSTP in the force-version, use the following command.

Command	Mode	Description
stp mst {enable disable}	Bridge	Enables/disables STP, RSTP or MSTP function.

Even though STP function does not operated, loop event does not occur in a switch which belongs to the non-dual path LAN environment.

8.3.5.2 Root Switch

To establish STP, RSTP, or MSTP function, first of all, root switch should be decided. In STP or RSTP, it is named as root switch and in MSTP it is as IST root switch. Each switch has its own bridge ID, and root switch on same LAN is decided by comparing their bridge ID. However, the user can modify root switch by configuring priority for it. The switch having the lowest priority is decided as root switch.

To change root switch by configuring priority for it, use the following command.

Command	Mode	Description
stp mst priority <i>MSTID-RANGE</i> <0-61440>	Bridge	Configures the priority of the switch: MSTID-RANGE: select instance number 0. 0-61440: priority value in steps of 4096 (default: 32768)
no stp mst priority <i>MSTID-RANGE</i>		Clears the Priority of the switch, enter the instance number.

8.3.5.3 Path-cost

After deciding root switch, you need to decide to which route you will forward the packet. To do this, the standard is path-cost.

Generally, path cost depends on transmission speed of LAN interface in the switch. The following table shows path cost according to transmit rate of LAN interface.

You can use same commands to configure STP and RSTP, but their path-costs are totally different. Please be careful not to make mistake.

Transmit Rate	Path-cost
4M	250
10M	100
100M	19
1G	4
10G	2

Tab. 8.2 STP Path-cost

Transmit Rate	Path-cost
4M	20,000,000
10M	2,000,000
100M	200,000
1G	20,000
10G	2,000

Tab. 8.3 RSTP Path-cost

When the route decided by path-cost gets overloading, you would better take another route. Considering these situations, it is possible to configure path-cost of root port so that user can configure route manually.

To configure path-cost, use the following command.

Command	Mode	Description
stp mst path-cost <i>MSTID-RANGE PORTS</i> <1-200000000>	Bridge	Sets the path-cost to configure route: MSTID_RANGE: select instance number (0-64). PORTS: select the port number. 1-200000000: enter the path cost value.
no stp mst path-cost <i>MSTID-RANGE PORTS</i>		Deletes the configured path-cost, enter the instance number and the port number.

8.3.5.4 Port-priority

When all conditions of two switches are same, the last standard to decide route is port-priority. It is also possible to configure port priority so that user can configure route manually. In order to configure port-priority, use the following command.

Command	Mode	Description
stp mst port-priority <i>MSTID-RANGE PORTS</i> <0-240>	Bridge	Configures port-priority.
no stp mst port-priority <i>MSTID-RANGE PORTS</i>		Disables port priority configuration.

8.3.5.5 MST Region

If MSTP is established in the hiD 6610 S311, decide which MST region the switch is going to belong to by configuring MST configuration ID. Configuration ID contains region name, revision, VLAN map.

To set configuration ID, use the following command.

Command	Mode	Description
stp mst config-id name <i>NAME</i>	Bridge	Designate the name for the region: name: set the MST region name. NAME: enter name to give the MST region.
stp mst config-id map <1-64> <i>VLAN-RANGE</i>		Configure the range of VLAN that is going to be grouping as a region: 1-64: select an instance ID number. VLAN-RANGE: enter a number of the VLANs to be mapped to the specified instance.
stp mst config-id revision <0-65535>		Configure the switches in the same MST boundary as same number: 0-65535: set the MST configuration revision number.



In case of configuring STP and RSTP, you don't need to configure configuration ID. If it is configured, error message is displayed.

To delete configuration ID, use the following command.

Command	Mode	Description
no stp mst config-id	Bridge	Delete the entire configured configuration ID.
no stp mst config-id name		Deletes the name of region, enter the MST region name.
no stp mst config-id map <1-64> [<i>VLAN-RANGE</i>]		Deletes entire VLAN-map or part of it, select the instance ID number and the number of the VLANs to remove from the specified instance.
no stp mst config-id revision		Deletes the configured revision number.

After configuring configuration ID in the hiD 6610 S311, you should apply the configuration to the switch. After changing or deleting the configuration, you must apply it to the switch. If not, it does not being injected into the switch.

To apply the configuration to the switch after configuring configuration ID, use the following command.

Command	Mode	Description
stp mst config-id commit	Bridge	Commits the configuration of the region.



After deleting the configured configuration ID, apply it to the switch using the above command.

8.3.5.6 MSTP Protocol

MSTP protocol has a backward compatibility. MSTP is compatible with STP and RSTP. If some other bridge runs with STP mode and send BPDU version of STP or RSTP, MSTP automatically changes to STP mode. STP mode can not be changed to MSTP mode automatically. If administrator wants to change network topology to MSTP mode, administrator has to clear previous detected protocol manually.

To configure the protocol, use the following command.

Command	Mode	Description
stp clear-detected-protocol <i>PORTS</i>	Bridge	Clears detected protocol and trys administrative protocol. PORTS: select the port number.

8.3.5.7 Point-to-point MAC Parameters

The internal sub layer service makes available a pair of parameters that permit inspection of, and control over, the administrative and operational state of the point-to-point status of the MAC entity by the MAC relay entity.

To configure the point-to-point status, use the following command.

Command	Mode	Description
stp point-to-point-mac <i>PORTS</i> {auto force-true force-false}	Bridge	Sets point-to-point MAC: PORTS: select the port number auto: auto detect force-true: force to point-to-point MAC force-false: force to shared MAC (not point to point MAC)

True means, the MAC is connected to a point-to-point LAN, i.e., there is at most one other system attached to the LAN. False means, the MAC is connected to a non point-to-point LAN, i.e., there can be more than one other system attached to the LAN.

To delete the point-to-point configuration, use the following command.

Command	Mode	Description
no stp point-to-point-mac <i>PORT</i>	Bridge	Deletes point-to-point MAC configuration: PORT: select the port number.

8.3.5.8 Edge Ports

Edge ports are used for connecting end devices. There are no switches or spanning-tree bridges after the edge port.

To configure edge port mode, use the following command.

Command	Mode	Description
stp edge-port <i>PORTS</i>	Bridge	Sets port edge mode: PORTS: select the port number.

To delete the edge port mode, use the following command.

Command	Mode	Description
no stp edge-port <i>PORTS</i>	Bridge	Deletes port edge mode: PORTS: select the port number.

8.3.5.9 Displaying Configuration

To display the configuration after configuring STP, RSTP, and MSTP, use the following command.

Command	Mode	Description
show stp	Enable Global Bridge	Shows the configuration of STP/RSTP/MSTP.
show stp mst		Shows the configuration when it is configured as MSTP.
show stp mst <i>MSTID-RANGE</i>		Shows the configuration of specific Instance, enter the instance number.
show stp mst <i>MSTID-RANGE</i> {all <i>PORTS</i> } [detail]		Shows the configuration of the specific Instance for the ports: MSTID_RANGE: select the MST instance number. all: select all ports. PORTS: select port number. detail: show detail information (as option).



In case STP or RSTP is configured in the SURPASS hiD 6610 S311, you should configure *MSTID-RANGE* as 0.

To display a configured MSTP of the switch, use the following command.

Command	Mode	Description
show stp mst config-id {current pending}	Enable Global Bridge	Shows the MSTP configuration identifier: current: shows the current configuration as it is used to run MST. pending: shows the edited configuration.



For example, after the user configures configuration ID, if you apply it to the switch with **stp mst config-id commit** command, you can check configuration ID with the **show stp mst config-id current** command.



However, if the user did not use the **stp mst config-id commit** command in order to apply to the switch after configuration, the configuration could be checked with the **show stp mst config-id pending** command.

8.3.6 Configuring PVSTP/PVRSTP

STP and RSPT are designed with one VLAN in the network. If a port becomes blocking state, the physical port itself is blocked. But PVSTP (Per VLAN Spanning Tree Protocol) and PVRSTP (Per VLAN Rapid Spanning Tree Protocol) maintains spanning tree instance for each VLAN in the network. Because PVSTP treats each VLAN as a separate network, it has the ability to load balance traffic by forwarding some VLANs on one trunk and other VLANs. PVRSTP provides the same functionality as PVSTP with enhancement.

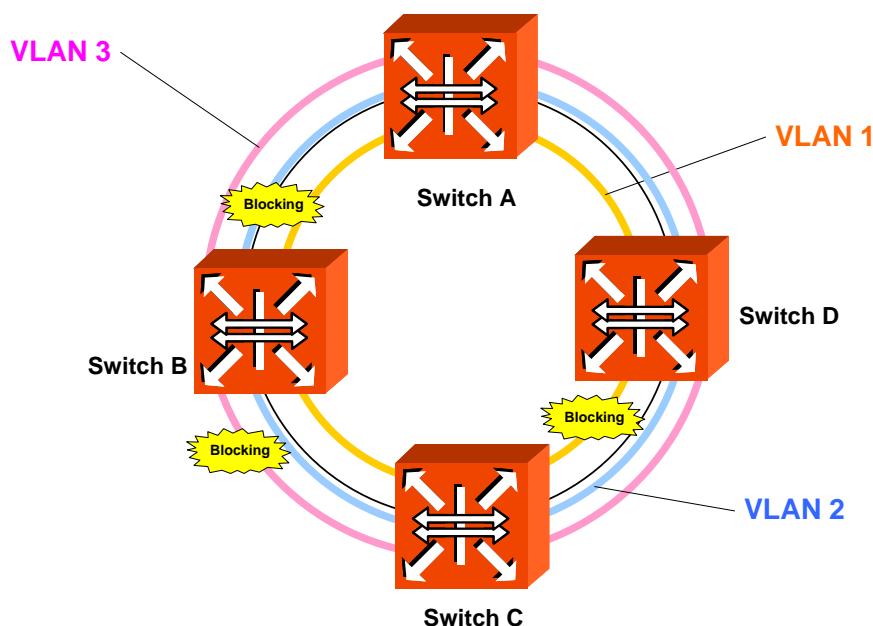


Fig. 8.24 Example of PVSTP

8.3.6.1 Activating PVSTP/PVRSTP

To configure PVSTP or PVRSTP, configure force-version in order to decide the mode. In order to decide force-version, use the following command.

Command	Mode	Description
stp pvst enable <i>VLAN-RANGE</i>	Bridge	Activates PVSTP or PVRSTP function. VLAN-RANGE : Vlan name

PVSTP is activated after selecting PVSTP in Force-version using the above command and PVRSTP is activated after selecting PVRSTP using the above commands. In PVSTP and PVRSTP, it is possible to configure only the current VLAN. If you input VLAN that does not exist, error message is displayed.

For the switches in LAN where dual path doesn't exist, Loop does not generate even though STP function is not configured. To disable configured PVSTP, PVRSTP, use the following command.

Command	Mode	Description
stp pvst disable	Bridge	Disables PVSTP or PVRSTP in VLAN.

8.3.6.2 Root Switch

In order establish PVSTP, PVRSTP function, first of all, Root switch should be decided. Each switch has its own Bridge ID and Root switch on same LAN is decided by comparing their Bridge ID. However, the user can change Root switch by configuring Priority for it. The switch having the lowest priority is decided as Root switch.

To change Root switch by configuring Priority for it, use the following command.

Command	Mode	Description
stp pvst priority <i>VLAN-RANGE</i> <0-61440>	Bridge	Configures a priority of switch.
no stp pvst priority <i>VLAN-RANGE</i>		Clears a priority of switch.

8.3.6.3 Path-cost

After deciding Root switch, you need to decide to which route you will forward the packet. To do this, the standard is path-cost. Generally, path-cost depends on transmission speed of LAN interface in switch. In case the route is overload based on Path-cost, it is better to take another route.

By considering the situation, the user can configure Path-cost of Root port in order to designate the route on ones own. To configure Path-cost, use the following command.

Command	Mode	Description
stp pvst path-cost <i>VLAN-RANGE PORTS</i> <1-200000000>	Bridge	Configures path-cost to configure route on user's own.
no stp pvst path-cost <i>VLAN-RANGE PORTS</i>		Clears path-cost configuration.

8.3.6.4 Port-priority

When all conditions of two switches are same, the last standard to decide route is port-priority. It is also possible to configure port priority so that user can configure route manually. To configure port priority, use the following command.

Command	Mode	Description
stp pvst port-priority <i>VLAN-RANGE PORTS</i> <0-240>	Bridge	Configures port-priority.
no stp pvst port-priority <i>VLAN-RANGE PORTS</i>		Disables port priority configuration.

8.3.7 Root Guard

The standard STP does not allow the administrator to enforce the position of the root bridge, as any bridge in the network with lower bridge ID will take the role of the root bridge. Root guard feature is designed to provide a way to enforce the root bridge placement in the network. Even if the administrator sets the root bridge priority to zero in an effort to secure the root bridge position, there is still no guarantee against bridge with priority zero and a lower MAC address.

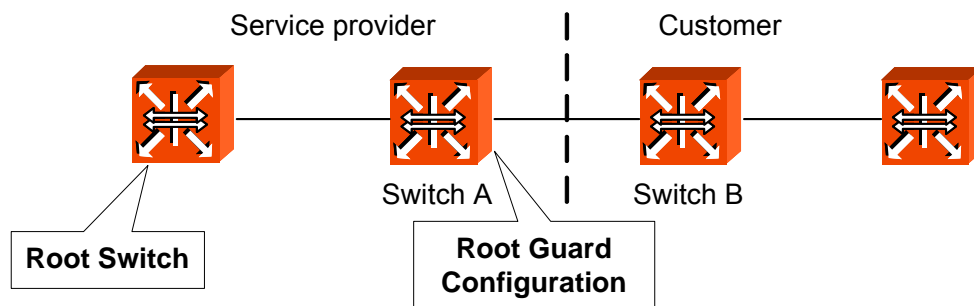


Fig. 8.25 Root Guard

Software-based bridge applications launched on PCs or other switches connected by a customer to a service-provider network can be elected as root switches. If the priority of bridge B is zero or any value lower than that of the root bridge, device B will be elected as a root bridge for this VLAN. As a result, network topology could be changed. This may lead to sub-optimal switching. But, by configuring root guard on switch A, no switches behind the port connecting to switch A can be elected as a root for the service provider's switch network. In which case, switch A will block the port connecting switch B.

To configure Root-Guard, use the following command.

Command	Mode	Description
stp pvst root-guard <i>VLAN-RANGE PORTS</i>	Bridge	Configures Root Guard on PVST network.
stp mst root-guard <i>MSTID-RANGE PORTS</i>		Configures Root Guard on MST network.
no stp pvst root-guard <i>VLAN-RANGE PORTS</i>		Disables Root Guard.
no stp mst root-guard <i>MSTID-RANGE PORTS</i>		

8.3.8 Restarting Protocol Migration

There are two switches which configured as STP and RSTP. Usually, in this case, STP protocol is used between two switches. But if someone configures the STP switch to RSTP mode, what happens? Because the RSTP switch already received STP protocol packet, the two switches still can work with STP mode even though RSTP is enabled at both. If you enable this command, the switch checks STP protocol packet once again.

To clear configured Restarting Protocol Migration, use the following command.

Command	Mode	Description
stp clear-detected-protocol <i>PORTS</i>	Bridge	Configures restarting protocol migration function.

8.3.9 Bridge Protocol Data Unit Configuration

Bridge Protocol Data Unit (BPDU) is a transmission message in LAN in order to configure, maintain the configuration for STP/RSTP/MSTP. Switches that STP is configured exchange their information BPDU to find best path. MSTP BPDU is general STP BPDU having additional MST data on its end. MSTP part of BPDU does not rest when it is out of Region.

- **Hello Time**
Hello time decides an interval time when a switch transmits BPDU. It can be configured from 1 to 10 seconds. The default is 2 seconds.
- **Max Age**
Root switch transmits new information every time based on information from another switches. However, if there are many switches on network, it takes lots of time to transmit BPDU. And if network status is changed while transmitting BPDU, this information is useless. To get rid of useless information, max age is identified in each information.
- **Forward Delay**
Switches find location of another switches connected to LAN though received BPDU and transmit packets. Since it takes certain time to receive BPDU and find the location before transmitting packet, switches send packet at regular interval. This interval time is named forward delay.



The configuration for BPDU is applied as selected in force-version. The same commands are used for STP, RSTP, MSTP, PVSTP and PVRSTP.

8.3.9.1 Hello Time

Hello time decides an interval time when a switch transmits BPDU. To configure hello time, use the following command.

Command	Mode	Description
stp mst hello-time <1-10>	Bridge	Configures hello time to transmit the message in STP, RSTP and MSTP: 1-10: set the hello time. (default: 2)
stp pvst hello-time <i>VLAN-RANGE</i> <1-10>		Configures hello time to transmit the message in PVSTP and PVRSTP: 1-10: set the hello time. (default: 2)

To clear configured hello-time, use the following command.

Command	Mode	Description
no stp mst hello-time	Bridge	Returns to the default hello time value of STP, RSTP and MSTP.
no stp pvst hellow-time <i>VLAN-RANGE</i>		Returns to the default hello time value of PVSTP and PVRSTP.

8.3.9.2 Forward Delay

It is possible to configure forward delay, which means time to take port status from listening to forwarding. To configure forward delay, use the following command.

Command	Mode	Description
stp mst forward-delay <4-30>	Bridge	Modifies forward-delay in STP, RSTP or MSTP, enter a delay time value. (default: 15)
stp pvst forward-delay <i>VLAN-RANGE</i> <4-30>		Modifies forward-delay in PVSTP and PVRSTP, enter a delay time value of VLAN. (default: 15)

To delete a configured forward delay, use the following command.

Command	Mode	Description
no stp mst forward-delay	Bridge	Returns to the default value of STP, RSTP and MSTP.
no stp pvst forward-delay <i>VLAN-RANGE</i>		Returns to the default value of PVSTP and PVRSTP per VLAN.

8.3.9.3 Max Age

Max age shows how long path message is valid. To configure max age to delete useless messages, use the following command.

Command	Mode	Description
stp mst max-age <6-40>	Bridge	Configures max age of route message of STP, RSTP or MSTP, enter a max age time value. (default: 20)
stp pvst max-age <i>VLAN-RANGE</i> <6-40>		Configures max age of route message of PVSTP, PVRSTP, enter a max age time value of VLAN. (default: 20)



It is recommended that max age is configured less than twice of forward delay and more than twice of hello time.

To delete a configured max age, use the following command.

Command	Mode	Description
no stp mst max-age	Bridge	Returns to the default max-age value of STP, RSTP and MSTP.
no stp pvst max-age <i>VLAN-RANGE</i>		Returns to the default max-age value of PVSTP and PVRSTP.

8.3.9.4 BPDU Hop

In MSTP, it is possible to configure the number of hop in order to prevent BPDU from wandering. BPDU passes the switches as the number of hop by this function.

To configure the number of hop of BPDU in MSTP, use the following command.

Command	Mode	Description
stp mst max-hops <1-40>	Bridge	Configures the number of hop for BPDU, set the number of possible hops in the region.
no stp mst max-hops		Deletes the number of hop for BPDU in MSTP.

8.3.9.5 BPDU Filter

BPDU filtering allows you to avoid transmitting on the ports that are connected to an end system. If the BPDU Filter feature is enabled on the port, then incoming BPDUs will be filtered and BPDUs will not be sent out of the port. To set the BPDU filter on the port, use the following command.

Command	Mode	Description
stp bpdu-filter {enable disable} <i>PORTS</i>	Bridge	Forbids all STP BPDUs to go out the specific port and not to recognize incoming STP BPDUs the specific port.

By default, it is disabled. The BPDU filter-enabled port acts as if STP is disabled on the port. This feature can be used for the ports that are usually connected to an end system or the port that you don't want to receive and send unwanted BPDU packets. Be cautious about using this feature on STP enabled uplink or trunk port. If the port is removed from VLAN membership, correspond BPDU filter will be automatically deleted.

8.3.9.6 BPDU Guard

BPDU guard has been designed to allow network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports with STP enabled are not allowed to influence the STP topology. This is achieved by disabling the port upon receipt of BPDU. This feature prevents Denial of Service (DoS) attack on the network by permanent STP recalculation. That is caused by the temporary introduction and subsequent removal of STP devices with low (zero) bridge priority.

To configure BPDU guard in the switch, perform the following procedure.

Step 1

Configure the specific port as edge-port.

Command	Mode	Description
stp edge-port <i>PORTS</i>	Bridge	Configures the port as Edge port.
no stp edge-port <i>PORTS</i>		Disables Edge port configuration.

Step 2

Configure BPDU Guard.

Command	Mode	Description
stp bpdu-guard	Bridge	Configures BPDU Guard function on switch.
no stp bpdu-guard		Disables BPDU Guard function.

However, BPDU Guard can be corrupted by unexpected cause. In this case, the edge port is blocked immediately and remains at this state until user recovers it. To prevent this problem, the hiD 6610 S311 switch provides BPDU guard auto-recovery function. When an edge port is down for BPDU packet which came from other switch, the port is recovered automatically after configured time.

To configure BPDU Guard auto-recovery, use the following command.

Command	Mode	Description
stp bpdu-guard auto-recovery	Bridge	Configures BPDU Guard auto-recovery on switch.
stp bpdu-guard auto-recovery-time <10-1000000>		Configures BPDU Guard auto-recovery-time.
no stp bpdu-guard auto-recovery		Disables BPDU Guard auto-recovery function.
no stp bpdu-guard auto-recovery-time		

To recover a blocked port by manually, use the following command.

Command	Mode	Description
stp bpdu-guard err-recovery <i>PORTS</i>	Bridge	Recovers a blocked port by manually.

8.3.9.7 Self Loop Detection

Although there is no double path in user's equipment, loop can be caused by network environment and cable condition connected to equipment. To prevent this, the hiD 6610 S311 has self loop detection to perceive that outgoing packet is got back. Through the self loop detection, you can prevent packet, which comes back because it blocks the port.

To enable/disable self loop detection, use the following command.

Command	Mode	Description
self-loop-detect {enable disable}	Bridge	Enables/disables self loop detection function.

To display a configuration for BPDU, use the following command.

Command	Mode	Description
show self-loop-detect	Enable	Shows status of self loop detection and a port where loop is happed.
show self-loop-detect {all PORTS}	Global Bridge	Shows self loop detection status on specified ports: all: all the ports PORTS: selected port

8.3.9.8 Displaying BPDU Configuration

To display the configuration for BPDU, use the following command.

Command	Mode	Description
show stp mst <i>MSTID-RANGE</i> {all PORTS} [detail]	Enable Global Bridge	Shows a configuration for BPDU for STP, RSTP and MSTP.
show stp mst <i>MSTID-RANGE</i> all [detail]		
show stp mst <i>MSTID-RANGE</i> PORTS [detail]		
show stp pvst <i>VLAN-RANGE</i> [all PORTS] [detail]		Shows a configuration for BPDU for PVSTP and PVRSTP.

8.3.10 Sample Configuration

Backup Route

When you design layer 2 network, you must consider backup route for stable STP network. This is to prevent network corruption when just one additional path exists.

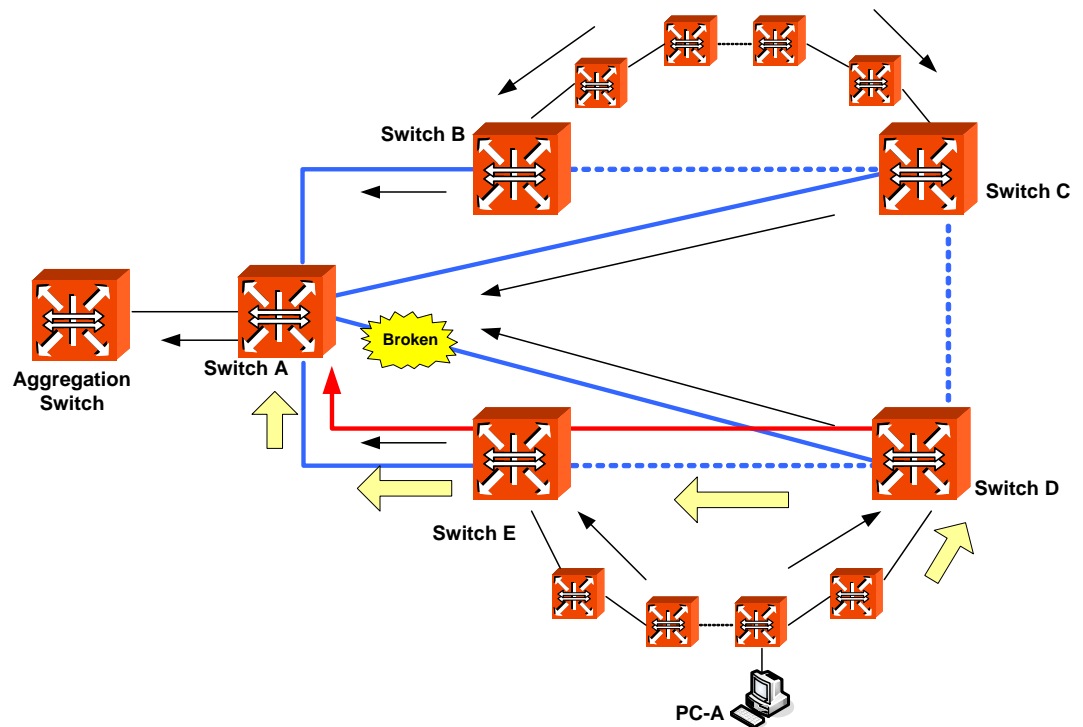
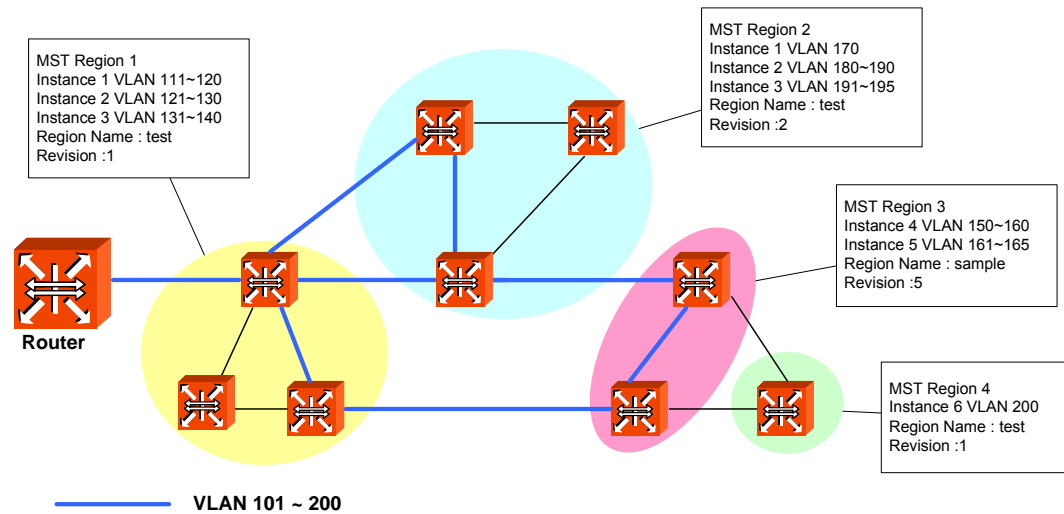


Fig. 8.26 Example of Layer 2 Network Design in RSTP Environment

In ordinary case, data packets go to Root switch A through the blue path. The black arrows describe the routine path to the Aggregation Switch. And the dot lines are in blocking state. But if there is a broken between Switch A and Switch B, the data from PC-A should find another route at Switch D. Switch D can send the data to Switch C and Switch E. Because Switch E has shorter hop count than Switch B, the data may go through the Switch E and A as the red line. And we can assume Switch E is also failed at the same time. In this case, since Switch D can has the other route to Switch C, the network can be stable than just one backup route network.

MSTP Configuration**Fig. 8.27** Example of Layer 2 Network Design in MSTP Environment

The following is an example of configuring MSTP in the switch.

```
SWITCH(bridge)# stp force-version mstp
SWITCH(bridge)# stp mst enable
SWITCH(bridge)# stp mst config-id map 2 1-50
SWITCH(bridge)# stp mst config-id name 1
SWITCH(bridge)# stp mst config-id revision 1
SWITCH(bridge)# stp mst config-id commit
SWITCH(bridge)# show stp mst

Status                enabled
bridge id              8000.00d0cb000183
designated root         8000.00d0cb000183
root port              0                path cost 0
max age                20.00            bridge max age        20.00
hello time             2.00             bridge hello time      2.00
forward delay          15.00            bridge forward delay    15.00
CIST regional root     8000.00d0cb000183  CIST path cost         0
max hops               20
name                   TEST
revision               1
instance vlans
-----
CIST      51-4094
  2       1-50
-----

SWITCH(bridge)#
```


8.4 VRRP (Virtual Router Redundancy Protocol)

VRRP (Virtual Router Redundancy Protocol) is configuring Virtual router (VRRP Group) consisted of VRRP routers to prevent network failure caused by one dedicated router. You can configure maximum 255 VRRP routers in VRRP group of hiD 6610 S311.

First of all, you need to decide the router which plays a roll as Master Virtual Router. The other routers will be Backup Virtual Routers. After you give the priority to these backup routers, the routers serve for Master Virtual Router when there are some problems in Master Virtual router. After you configure VRRP, configure all routers in VRRP with unified Group ID and assign unified Associated IP address to them. After that, decide Master Virtual Router and Backup Virtual Router. A router which has the highest priority is supposed to be Master and Backup Virtual Routers also get orders depending on priority.

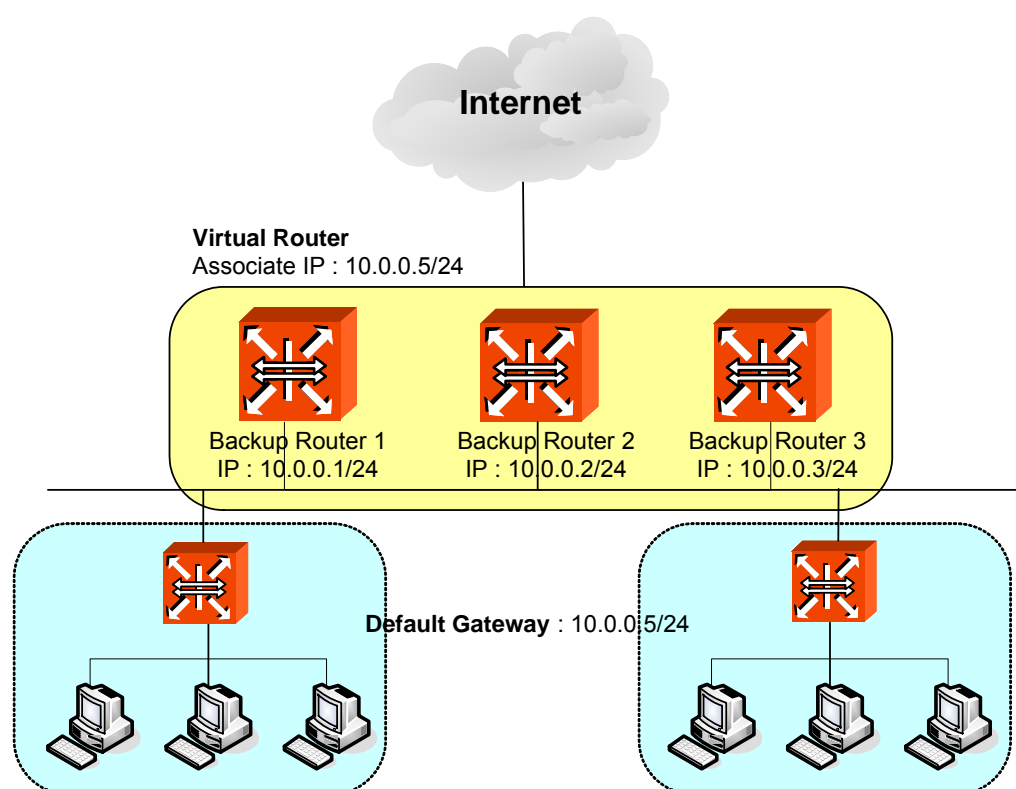


Fig. 8.28 VRRP Operation

In case routers have same priorities, then a router, which has lower IP address, gets the precedence. The Fig. 8.28 shows an example of configuring three routers which have IP addresses, 10.0.0.1/24, 10.0.0.2/24 and 10.0.0.3/24 for each one as Virtual router by Associated IP, 10.0.0.5/24. If these three routers have same Priority, a router, which has the smallest IP, address, 10.0.0.1/24 is decided to be Master Router. Also, switches and PCs connected to the Virtual Router are to have IP address of Virtual Router, 10.0.0.5/24 as default gateway.

8.4.1 Configuring VRRP

To configure the hiD 6610 S311 as device in Virtual Router, use the following command on *Global Configuration* mode. Then you can configure VRRP by opening *VRRP Configuration* mode.

Command	Mode	Description
router vrrp <i>INTERFACE</i> <i>GROUP-ID</i>	Global	Configures Virtual Router (VRRP Group). GROUP ID : 1-255

To display a configuration of VRRP, use the following command.

Command	Mode	Description
show vrrp	Enable Global	Shows current configuration of VRRP.
show vrrp interface <i>INTERFACE</i>		Shows current configuration of specified interface VRRP.

To return to *Global Configuration* mode or *Privileged EXEC Enable* mode, use the following commands.

Command	Mode	Description
exit	VRRP	Returns to <i>Global Configuration</i> mode.
end		Goes back right to <i>Privilege EXEC</i> mode.

To delete the VRRP configuration, use the following command.

Command	Mode	Description
no router vrrp <1-255>	Global	Configures Virtual Router (VRRP Group). 1-255: group ID

8.4.1.1 Associated IP Address

After configuring Virtual Router, you need to assign Associated IP address in Virtual Router. Assign unified IP address to routers in one Group.

To assign Associate IP address to routers in Virtual Router or delete configured Associate IP address, use the following command.

Command	Mode	Description
associate <i>IP-ADDRESS</i>	VRRP	Assigns an associated IP address to Virtual Router.
no associate <i>IP-ADDRESS</i>		Deletes an assigned associated IP address to Virtual Router.

The following is an example of assigning IP address, 10.0.0.5 to Virtual Router.

```
SWITCH(config-router)# associate 10.0.0.5
SWITCH(config-router)#
```

8.4.1.2 Access to Associated IP Address

If you configure the function of accessing Associated IP address, you can access to Associated IP address by the commands such as ping.

To configure the function of accessing Associated IP address, use the following command.

Command	Mode	Description
vip-access [enable disable]	VRRP	Configures the function of accessing associated IP address.

8.4.1.3 Master Router and Backup Router

The hiD 6610 S311 can be configured as Master Router and Backup Router by comparing Priority and IP address of devices in Virtual Router. First of all, it compares Priority. A device, which has higher Priority, is to be higher precedence. And when devices have same Priority, then it compares IP address. A device, which has lower IP address, is to be higher precedence. If a problem occurs on Master Router and there are more than two routers, one of them is selected as new Master Router according to their precedence.

To configure Priority of Virtual Router or delete the configuration, use the following commands.

Command	Mode	Description
vr-priority <1-254>	VRRP	Configures Priority of Virtual Router. 1-254: VRRP priority number (default: 100)
no vr-priority		Deletes configured Priority of Virtual Router.



Priority of Virtual Backup Router can be configured from 1 to 254.

To set VRRP timers or delete the configuration, use the following command.

Command	Mode	Description
vr-timers advertisement <1-10>	VRRP	Sets VRRP timers. 1-10: advertisement time in the unit of second
no vr-timers advertisement		Clears a configured VRRP time.

The following is an example of configuring Master Router and Backup Router by comparing their Priorities: Virtual Routers, Layer 3 SWITCH 1 – 101 and Layer 3 SWITCH 2 – 102. Then, regardless of IP addresses, one that has higher Priority, Layer 3 SWITCH 2 becomes Master Router.

<Layer 3 SWITCH1: IP Address - 10.0.0.1/24>

```
SWITCH1(config)# router vrrp default 1
SWITCH1(config-router)# associate 10.0.0.5
SWITCH1(config-router)# vr_priority 101
SWITCH1(config-router)# exit
SWITCH1(config)# show vrrp

default - virtual router 1
-----
state                backup
virtual mac address   00:00:5E:00:01:01
advertisement interval 1 sec
preemption            enabled
priority              101
master down interval  3.624 sec
[1] associate address : 10.0.0.5
```

<Layer 3 SWITCH 2: IP Address - 10.0.0.2/24>

```
SWITCH2(config)# router vrrp default 1
SWITCH2(config-router)# associate 10.0.0.5
SWITCH1(config-router)# vr_priority 102
SWITCH2(config-router)# exit
SWITCH2(config)# show vrrp

default - virtual router 1
-----
state                master
virtual mac address   00:00:5E:00:01:01
advertisement interval 1 sec
preemption            enabled
priority              102
master down interval  3.620 sec
[1] associate address : 10.0.0.5
```

SWITCH 2 with higher priority
is configured as Master.

By default, Priority of hiD 6610 S311 is configured as “100”. So, unless you configure specific Priority, this switch becomes Master Router because a device, which has lower IP address, has higher precedence.

Also, when there are more than two Backup Routers, IP addresses are compared to decide order. The following is an example of configuring Master Router and Backup Router by comparing IP addresses: Virtual Routers, Layer 3 SWITCH 1 – 10.0.0.1 and Layer 3 SWITCH 2 – 10.0.0.2.

<Layer 3 SWITCH1: IP address - 10.0.0.1/24>

```
SWITCH1(config)# router vrrp default 1
SWITCH1(config-router)# associate 10.0.0.5
SWITCH1(config-router)# exit
SWITCH1(config)# show vrrp

default - virtual router 1
-----
state                master
virtual mac address   00:00:5E:00:01:01
advertisement interval 1 sec
preemption            enabled
priority              100
master down interval   3.624 sec
[1] associate address : 10.0.0.5
```

<Layer 3 SWITCH 2: IP Address - 10.0.0.2/24>

```
SWITCH2(config)# router vrrp default 1
SWITCH2(config-router)# associate 10.0.0.5
SWITCH2(config-router)# exit
SWITCH2(config)# show vrrp

default - virtual router 1
-----
state                backup
virtual mac address   00:00:5E:00:01:01
advertisement interval 1 sec
preemption            enabled
priority              100
master down interval   3.620 sec
[1] associate address : 10.0.0.5
```

In case of same priorities,
SWITCH 1 with lower IP
address is configured as
Master.

8.4.1.4 VRRP Track Function

When the link connected to Master Router of VRRP is off as below, if link of Master Router is not recognized, the users on the interface are not able to communicate because the interface is not able to access to Master Router.

In the condition that Link to VRRP's master router is down as the figure shown below, or the link of Master Router cannot be recognized, the communication would be impossible.

For the hiD 6610 S311, you can configure Master Router to be changed by giving lower Priority to Master Router when the link of Mater Router is disconnected. This function is VRRP Track.

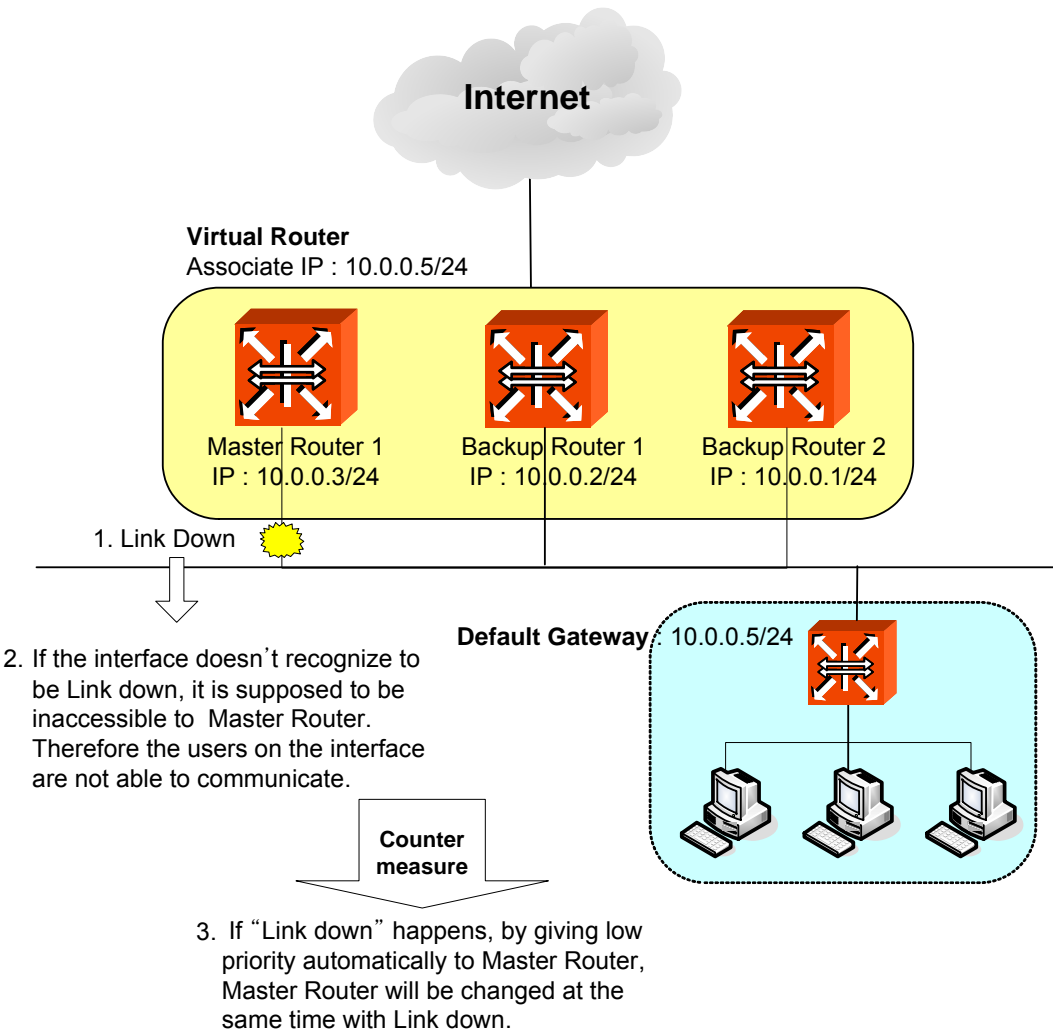


Fig. 8.29 VRRP Track

To configure VRRP Track, use the following command.

Command	Mode	Description
<code>track interface INTERFACE priority <1-254></code>	VRRP	Configures VRRP Track. The Priority becomes lower as the configured value.

To release VRRP Track configuration, use the following command.

Command	Mode	Description
<code>no track interface INTERFACE</code>	VRRP	Disables VRRP Track configuration.

8.4.1.5 Authentication Password

If anyone knows Group ID and Associated IP address, he can configure another device as a Virtual Router. To prevent this, user needs to configure a password, named authentication password that can be used only in Virtual Router user configured.

To configure an authentication password for security of Virtual Router, use the following command on VRRP configuration mode.

Command	Mode	Description
authentication clear_text <i>PASSWORD</i>	VRRP	Configures an authentication password.
no authentication		Deletes a configured authentication password.



Authentication password can be configured with maximum 7 digits.

The following is an example of configuring Authentication password in Virtual Router as network and showing it.

```
SWITCH(config-router)# authentication clear_text network
SWITCH(config-router)# show running-config
Building configuration...
(Omitted)
vrrp default 1
authentication clear_text network
associate 10.0.0.5
no snmp
SWITCH(config-router)#
```

8.4.1.6 Preempt

Preempt is a function that an added device with the highest Priority user gave is automatically configured as Master Router without rebooting or specific configuration when you add an other device after Virtual Router is configured.

To configure Preempt, use the following command on VRRP configuration mode.

Command	Mode	Description
preempt {enable disable}	VRRP	Enables or disables Preempt. (default: enable)

The following is an example of disabling Preempt.

```
SWITCH(config-vrrp)# preempt disable
SWITCH(config-vrrp)# exit
SWITCH(config)# show vrrp

default - virtual router 1
-----
state                master
virtual mac address   00:00:5E:00:01:01
advertisement interval 1 sec
preemption            disabled
priority              100
master down interval  3.624 sec
[1] associate address : 10.0.0.5

SWITCH(config)#
```

Also, to make Preempt “enable” as default setting, use the following command on VRRP configuration mode.

Command	Mode	Description
no preempt	VRRP	Deletes the former configuration of Preempt to enable it.

8.4.1.7 VRRP Statistics

To display the VRRP statistics that packets have been sent and received, use the following command.

Command	Mode	Description
show vrrp stat	Enable Global VRRP	Shows statistics of packets in Virtual Router Group.

The following is an example of viewing statistics of packets in Virtual Router Group.

```
SWITCH(config)# show vrrp stat
VRRP statistics :
VRRP packets rcvd with invalid TTL      0
VRRP packets rcvd with invalid version  0
VRRP packets rcvd with invalid VRID     0
VRRP packets rcvd with invalid size     0
VRRP packets rcvd with invalid checksum 0
VRRP packets rcvd with invalid auth-type 0
VRRP packets rcvd with interval mismatch 0

SWITCH(config)#
```

To clear the VRRP statistics information, use the following command.

Command	Mode	Description
clear vrrp stat	Global VRRP	Clears statistics of packets in Virtual Router Group.

8.5 Rate Limit

User can customize port bandwidth according to user's environment. By this configuration, you can prevent a certain port to monopolize whole bandwidth so that all ports can use bandwidth equally. Egress and ingress can be configured both to be same and to be different.

The hiD 6610 S311 can apply the rate limit and support ingress policing and egress shaping.

8.5.1 Configuring Rate Limit

To set a port bandwidth, use the following command.

Command	Mode	Description
rate <i>PORTS</i> <i>RATE</i> [egress ingress]	Bridge	Sets port bandwidth. If you input egress or ingress, you can configure outgoing packet or incoming packet. The unit is 64 Kbps.
no rate <i>PORTS</i>		Clears rate configuration of a specific port.
no rate <i>PORTS</i> [egress ingress]		Clears rate configuration of a specific port by transmitting direction.

Unless you input neither egress nor ingress, they are configured to be same. To switch, egress is incoming packet. To display the configured bandwidth, use the following command.

Command	Mode	Description
show rate	Global	Shows the configured bandwidth.

8.5.2 Sample Configuration

The following is an example of showing the configuration after setting the bandwidth of 64Mbps to port number 1 and 128Mbps to the port number 2.

```
SWTICH(bridge)# rate 1 64
SWTICH(bridge)# rate 2 128
SWTICH(bridge)# show rate
unit : kbps E : Enhanced
-----
Port | Ingress | Egress | Port | Ingress | Egress
-----+-----
  1 |    64   |    64   |  2 |    128   |    128
  3 |   N/A   |   N/A   |  4 |   N/A   |   N/A
  5 |   N/A   |   N/A   |  6 |   N/A   |   N/A
  7 |   N/A   |   N/A   |  8 |   N/A   |   N/A
(Omitted)
SWTICH(bridge)#
```

8.6 Flood Guard

Flood-guard limits number of packets, how many packets can be transmitted, in configured bandwidth, whereas Rate limit controls packets through configuring width of bandwidth, which packets pass through. This function prevents receiving packets more than configured amount without enlarging bandwidth.

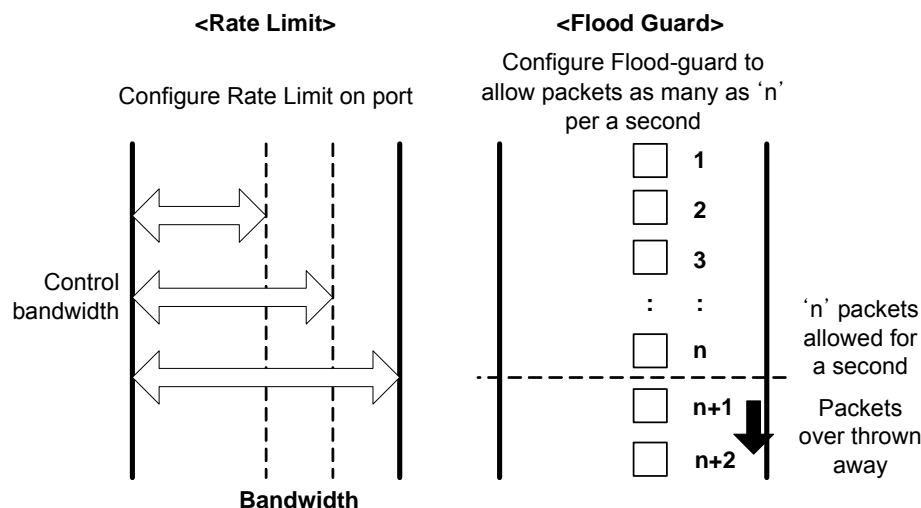


Fig. 8.30 Rate Limit and Flood Guard

8.6.1 Configuring Flood-Guard

To configure the number of packets, which can be transmitted in a second, use the following command.

Command	Mode	Description
mac-flood-guard PORTS <1-2000000>	Bridge	Limits the number of packets which can be transmitted to the port for 1 second.
no mac-flood-guard PORTS		Clears the configured Flood Guard.

To display a configuration of flood guard, use the following command.

Command	Mode	Description
show mac-flood-guard [macs]	Bridge	Shows the configured Flood Guard.

8.6.2 Sample Configuration

The following is an example of showing the configuration after limiting the number of packets transmitted to the port number 1 as 10,000.

```
SWITCH(bridge)# mac-flood-guard 1 10000
SWITCH(bridge)# show mac-flood-guard
-----
Port Rate(fps) | Port Rate(fps)
-----+-----
1    10000    | 2 Unlimited
```

```

3 Unlimited | 4 Unlimited
5 Unlimited | 6 Unlimited
7 Unlimited | 8 Unlimited
9 Unlimited | 10 Unlimited
11 Unlimited | 12 Unlimited
13 Unlimited | 14 Unlimited
15 Unlimited | 16 Unlimited

```

(Omitted)

SWITCH(bridge)#

8.7 Bandwidth

Routing protocol uses bandwidth information to measure routing distance value. To configure bandwidth of interface, use the following command.

Command	Mode	Description
bandwidth <i>BANDWIDTH</i>	Interface	Configures bandwidth of interface, enter the value of bandwidth.



The bandwidth can be from 1 to 10,000,000 Kbits. This bandwidth is for routing information implement and it does not concern physical bandwidth.

To delete a configured bandwidth, use the following command.

Command	Mode	Description
no bandwidth <i>BANDWIDTH</i>	Interface	Deletes configured bandwidth of interface, enter the value.

The following is an example of configuration to bandwidth as 1000.

```

SWITCH(config-if)# bandwidth 1000
SWITCH(config-if)# show running-config interface 1
!
interface default
    bandwidth 1m
    ip address 10.27.41.181/24
!
SWITCH(config-if)#

```

8.8 Dynamic Host Configuration Protocol (DHCP)

Dynamic host configuration protocol (DHCP) is a TCP/IP standard for simplifying the administrative management of IP address configuration by automating address configuration for network clients. The DHCP standard provides for the use of DHCP servers as a way to manage dynamic allocation of IP addresses and other related configuration details to DHCP-enabled clients on the network.

Every device on a TCP/IP network must have a unique IP address in order to access the network and its resources. The IP address (together with its related subnet mask) identifies both the host computer and the subnet to which it is attached. When you move a computer to a different subnet, the IP address must be changed. DHCP allows you to dynamically assign an IP address to a client from a DHCP server IP address database on the local network.

The DHCP provides the following benefits:

● Saving Cost

Numerous users can access the IP network with a small amount of IP resources in the environment that most users do not have to access the IP network at the same time all day long. This allows the network administrators to save the cost and IP resources.

● Effective Network Management

By deploying DHCP in a network, this entire process is automated and centrally managed. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it logs on to the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

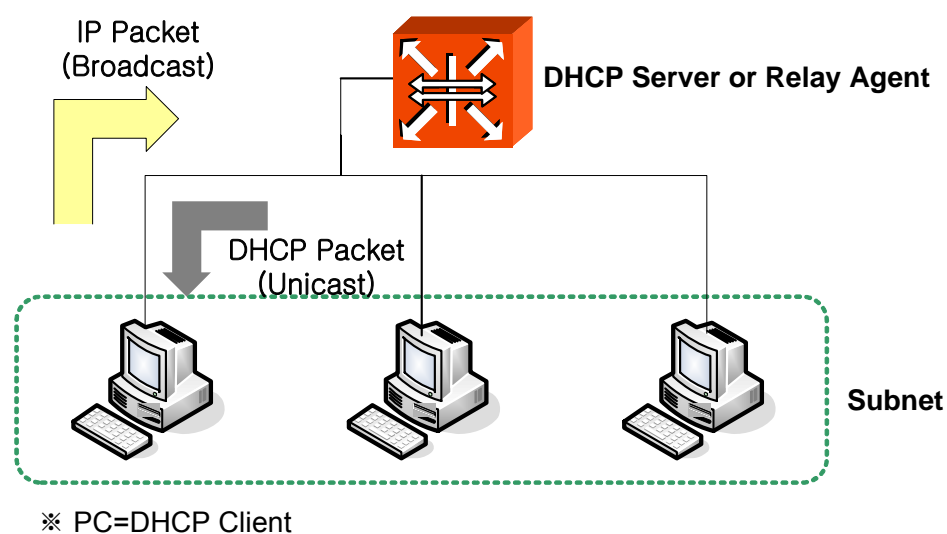


Fig. 8.31 DHCP Service Construction

8.8.1 DHCP Server

To provide DHCP server by configuring the switch as DHCP server, open *Global Configuration* mode.

To activate the DHCP Server in the system, use the following command.

Command	Mode	Description
ip dhcp active server	Global	Activates the switch as DHCP server.

To disable the DHCP server, use the following command.

Command	Mode	Description
no ip dhcp active server	Global	Disables the DHCP server function.

8.8.2 DHCP Pool

The DHCP pool is a group of IP addresses that will be assigned to DHCP clients by DHCP server. You can create various DHCP pools that can be configured with a different network, default gateway and range of IP addresses. This allows the network administrators to effectively handle multiple DHCP environments.

- DHCP Pool Creation
- DHCP Subnet
- Subnet Default Gateway
- IP Address Range
- IP Lease Time
- DNS Server
- Manual Binding
- Displaying Configuration
- Recognition of DHCP Client
- Lease Database Back-up & Reset

8.8.2.1 DHCP Pool Creation

In *Global Configuration* mode, you can create the IP pool.

To create DHCP Pool, use the following command.

Command	Mode	Description
ip dhcp pool <i>POOL-NAME</i>	Global	Creates a DHCP pool and open <i>DHCP Pool Configuration</i> mode.
no ip dhcp pool <i>POOL-NAME</i>		Deletes a created DHCP pool.

The following is an example of creating the DHCP pool as *sample*.

```
SWITCH(config)# ip dhcp pool sample
SWITCH(config-dhcp[sample])#
```

8.8.2.2 DHCP Subnet

To specify a subnet of the DHCP pool, use the following command.

Command	Mode	Description
subnet <i>A.B.C.D/M</i>	DHCP Pool	Specifies a subnet of the DHCP pool. A.B.C.D/M: network address



For the hiD 6610 S311, it is possible to specify several subnets in a single DHCP Pool.

To delete the DHCP subnet, use the following command.

Command	Mode	Description
no subnet <i>A.B.C.D/M</i>	DHCP Pool	Deletes a specified subnet.

8.8.2.3 Subnet Default Gateway

To specify a default gateway of the DHCP pool, use the following command.

Command	Mode	Description
default-gateway <i>A.B.C.D1</i> <i>A.B.C.D2 ... A.B.C.D8</i>	DHCP Pool	Specifies a default gateway of the DHCP pool. A.B.C.D: default gateway IP address

The following is an example for configuring subnet default gateway.

```
SWITCH(config)# ip dhcp pool test
SWITCH(config-dhcp[test])#
SWITCH(config-dhcp[test])# subnet 100.1.1.0/24
SWITCH(config-dhcp[test])# default-gateway 100.1.1.254
SWITCH(config-dhcp[test])#
```

To delete the configured default-gateway, use the following command.

Command	Mode	Description
no default-gateway <i>A.B.C.D</i>	DHCP Pool	Deletes a specified default gateway.
no default-gateway all		Deletes all the configured default-gateways.

8.8.2.4 IP Address Range

After configuring DHCP subnet, you need to configure IP address range used in the subnet. To configure IP address range, use the following command.

Command	Mode	Description
range <i>A.B.C.D1 A.B.C.D2</i>	DHCP Pool	Configures IP address range. A.B.C.D1: Start IP address A.B.C.D2: End IP address



You can also specify several inconsecutive ranges of IP addresses in a single DHCP pool, e.g. 100.1.1.1 to 100.1.1.62 and 100.1.1.129 to 100.1.1.190.



When specifying a range of IP address, the start IP address must be prior to the end IP address.

To delete the configured IP address range, use the following command.

Command	Mode	Description
no range <i>A.B.C.D1 A.B.C.D2</i>	DHCP Pool	Deletes the configured IP address range. A.B.C.D1: Start IP address A.B.C.D2: End IP address

8.8.2.5 IP Lease Time

Basically, the DHCP server leases an IP address in the DHCP pool to DHCP clients, which will be automatically returned to the DHCP pool when it is no longer in use or expired by IP lease time.

To specify IP lease time, use the following command.

Command	Mode	Description
lease-time default <120-2147483637>	DHCP Pool	Sets default IP lease time in the unit of second. (default: 3600)
lease-time max <120-2147483637>		Sets maximum IP lease time in the unit of second. (default: 3600)

The default is one hour (3600 seconds), and the maximum is two hours. And the configuration is applicable only to appropriate IP Pool.

To delete configured lease time, use the following command.

Command	Mode	Description
no lease-time {default max}	DHCP Pool	Deletes specified IP lease time.

8.8.2.6 DNS Server

To specify a DNS server to inform DHCP clients, use the following command.

Command	Mode	Description
dns-server <i>A.B.C.D1</i> [<i>A.B.C.D2</i>] [<i>A.B.C.D3</i>]	DHCP Pool	Specifies a DNS server. Up to 3 DNS servers are possible. A.B.C.D: DNS server IP address
no dns-server <i>A.B.C.D1</i> [<i>A.B.C.D2</i>] [<i>A.B.C.D3</i>]		Deletes a specified DNS server.
no dns-server all		Deletes all the specified DNS servers.



If you want to specify a DNS server for all the DHCP pools, use the **dns server** command. For more information, see Section 6.1.8.

8.8.2.7 Manual Binding

To manually assign a static IP address to a DHCP client who has a specified MAC address, use the following command.

Command	Mode	Description
fixed-address <i>A.B.C.D</i> <i>MACADDR</i>	DHCP Pool	Assigns a static IP address to a DHCP client. A.B.C.D: static IP address MACADDR: MAC address

To delete the fixed-address, use the following command.

Command	Mode	Description
no fixed-address <i>A.B.C.D</i>	DHCP Pool	Deletes a specified static IP assignment

8.8.2.8 Recognition of DHCP Client

Actually, the hiD 6610 S311 DHCP server is supposed to prohibit assigning IP address when DHCP packets have no CID. However, Linux client sends discover message without CID. For this reason, hiD 6610 S311 is added the condition of DHCP server which it can assign IP address without CID. In hardware-address option, the switch decides IP assignment based on MAC address only without checking particular CID, but in client-ID option, the switch checks MAC address and particular client ID to assign IP address.

Use the following command to configure DHCP server for checking the MAC address or CID.

Command	Mode	Description
ip dhcp database-key { <i>client-id</i> <i>hardware-address</i> }	Global	Configures to recognize a client with a client ID only or both of hardware address and CID.

8.8.2.9 Authorized ARP

DHCP Authorized ARP is to limit the leasing of IP addresses to authorized users. It can

be strength security by blocking ARP responses from unauthorized users at the DHCP server.

The following is the commands of blocking the user who uses IP address as fixed.

Command	Mode	Description
ip dhcp authorized-arp {default-lease-time half-lease-time max-lease-time}	Global	Enables dynamic ARP learning.
no ip dhcp authorized-arp		Disables dynamic ARP learning.

You can check the information of valid IP and invalid IP after enabling authorized ARP function using the following command.

Command	Mode	Description
show ip dhcp authorized-arp valid	Enable	Shows the assigned IP addresses through the proper process.
show ip dhcp authorized-arp invalid	Global	Shows MAC address using the fixed IP and the used IP address and the time of blocking IP address.

To clear the data of fixed IP, use the following command.

Command	Mode	Description
clear ip dhcp authorized-arp invalid	Enable Global Bridge	Deletes a data of fixed IP.

8.8.2.10 Displaying Configuration

To display DHCP pool configuration, use the following command.

Command	Mode	Description
show ip dhcp pool [POOL-NAME]	Enable	Shows IP Pool configuration.
show ip dhcp pool summary [POOL-NAME]	Global Bridge	Shows IP addresses assigned from DHCP of each IP pool.

To display lease data of IP address which is assigned to the IP Pool, use the following command.

Command	Mode	Description
show ip dhcp lease {all bound abandon offer fixed free} [POOL-NAME]	Enable Global Bridge	Shows the list of assigned IP address. all: all IP addresses bound: assigned IP address abandon: illegally assigned IP address offer: IP address being ready to be assigned fixed: manually assigned IP address free: remaining IP address
show ip dhcp lease detail [/IP-ADDRESS]		

8.8.3 Registering Global DNS Server

User is able to register not only DNS server that is applied whole DHCP pools in *Global Configuration Mode* but also DNS server configured in particular *DHCP Pool* configuration mode.

To register the DNS server of entire DHCP Pools globally, use the following command,.

Command	Mode	Description
ip dhcp default-config dns-server <i>IP-ADDRESS1</i> [<i>IP-ADDRESS2</i>] [<i>IP-ADDRESS3</i>]	Global	Registers the basic DNS server of all DHCP Pools.

To remove the registered DNS server, use the following command.

Command	Mode	Description
no ip dhcp default-config dns-server <i>IP-ADDRESS</i>	Global	Deletes the global DNS server.
no ip dhcp default-config dns-server		

8.8.4 Setting global lease Time

User is able to set not only lease time that is applied whole DHCP pools in *Global Configuration Mode* but also lease time configured in particular *DHCP Pool* configuration mode.

To set the global lease time of entire DHCP Pools, use the following command,.

Command	Mode	Description
ip dhcp default-config lease-time default <i>TIME</i>	Global	Sets the lease time to use IP address. TIME: 120-2147483637 (Default: 3600 seconds)
ip dhcp default-config lease-time max <i>TIME</i>		Sets the maximum lease time to use IP address. TIME: 120-2147483637 (Default: 3600 seconds)

To delete the configured lease time, use the following command.

Command	Mode	Description
no ip dhcp default-config lease-time default	Global	Deletes the configured lease time.
no ip dhcp default-config lease-time max		

8.8.5 DHCP Relay Agent

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. The DHCP relay agents are used to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. The DHCP relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently.

By contrast, DHCP relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The DHCP relay agent sets the gateway address and, if configured, adds the DHCP option 82 information in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing the DHCP option 82 information.

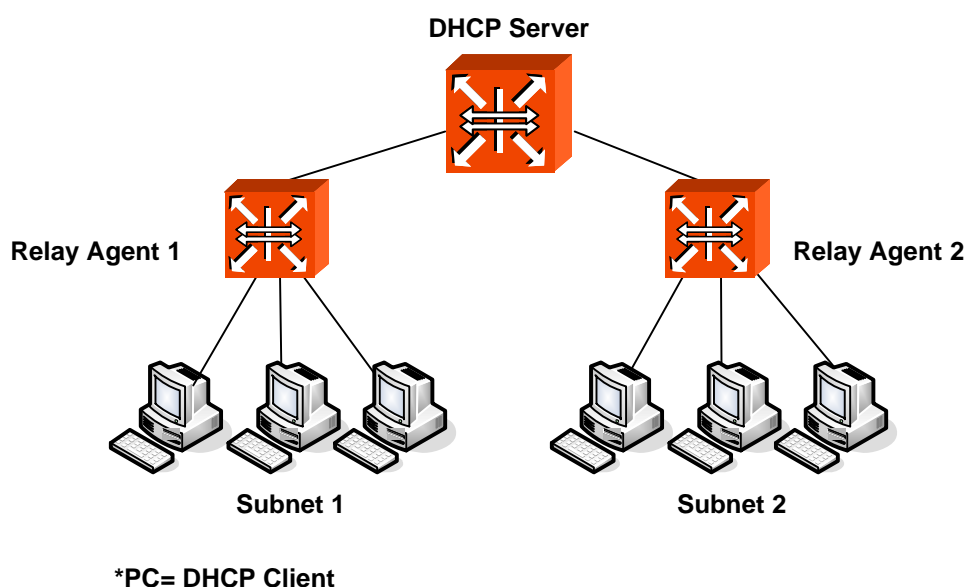


Fig. 8.32 Example of DHCP Relay Agent

8.8.5.1 Enable DHCP Relay Agent

To configure the hiD 6610 S311 as a relay agent, use the following command in *Global Configuration* mode.

Command	Mode	Description
<code>ip dhcp active relay <1-4094> A.B.C.D</code>	Global	Registers DHCP server and configures the switch as a relay agent. A.B.C.D : IP address of DHCP server VENDOR-ID: Vendor ID (e.g. XX:XX:XX)
<code>ip dhcp active relay <1-4094> VENDOR-ID A.B.C.D</code>		

To delete registered DHCP server and release the relay agent configuration, use the following command,

Command	Mode	Description
<code>no ip dhcp active relay <1-4094>.SERVERS</code>	Global	Delete DHCP server and release the switch as a relay agent.
<code>no ip dhcp active relay all</code>		Deletes all of the registered DHCP servers and the switch as a relay agent.

8.8.5.2 Smart Relay Agent Forwarding

If there is no DHCP offer message from a DHCP server, the DHCP relay agent switches the gateway address to secondary address. To help DHCP relay agent switch gateway address to secondary address, you need to enable DHCP smart-relay function. Use the following command.

Command	Mode	Description
<code>ip dhcp smart-relay</code>	Global	Makes DHCP relay agent to switch gateway address to secondary address automatically.
<code>no ip dhcp smart-relay</code>		Disables smart-relay function.

8.8.6 DHCP Option-82

In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using the DHCP option 82, a DHCP relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP relay agent will automatically add the circuit ID and the remote ID to the option 82 field in the DHCP packets and forward them to the DHCP server.

The DHCP option 82 resolves the following issues in an environment in which untrusted hosts access the internet via a circuit based public network:

Broadcast Forwarding

The DHCP option 82 allows a DHCP relay agent to reduce unnecessary broadcast flooding by forwarding the normally broadcasted DHCP response only on the circuit indicated in the circuit ID.

DHCP Address Exhaustion

In general, a DHCP server may be extended to maintain a DHCP lease database with an IP address, hardware address and remote ID. The DHCP server should implement policies that restrict the number of IP addresses to be assigned to a single remote ID.

Static Assignment

A DHCP server may use the remote ID to select the IP address to be assigned. It may permit static assignment of IP addresses to particular remote IDs, and disallow an address request from an unauthorized remote ID.

IP Spoofing

A DHCP client may associate the IP address assigned by a DHCP server in a forwarded DHCP ACK message with the circuit to which it was forwarded. The circuit access device may prevent forwarding of IP packets with source IP addresses, other than, those it has associated with the receiving circuit. This prevents simple IP spoofing attacks on the central LAN, and IP spoofing of other hosts.

MAC Address Spoofing

By associating a MAC address with a remote ID, a DHCP server can prevent offering an IP address to an attacker spoofing the same MAC address on a different remote ID.

Client Identifier Spoofing

By using the agent-supplied remote ID option, the untrusted and as-yet unstandardized client identifier field need not be used by the DHCP server.

Fig. 8.33 shows how the DHCP relay agent with the DHCP option 82 operates.

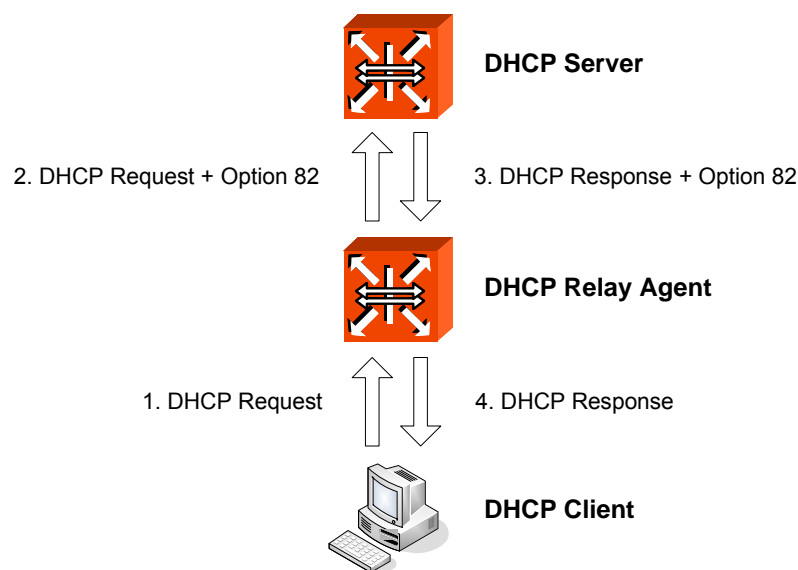


Fig. 8.33 DHCP Option 82 Operation

8.8.6.1 Enabling DHCP Option-82

To enable/disable DHCP option-82 in the hiD 6610 S311, use the following command.

Command	Mode	Description
<code>ip dhcp option82</code>	Global	Enables the system to add the DHCP option 82 field.
<code>no ip dhcp option82</code>		Disables the system to add the DHCP option 82 field.

8.8.6.2 Option 82 Sub-Option

The DHCP option 82 enables a DHCP relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement security and IP address assignment policies.

There are 2 sub-options for the DHCP option 82 information as the follows:

- **Remote ID**
This sub-option may be added by DHCP relay agents which terminate switched or permanent circuits and have mechanisms to identify the remote host of the circuit. Note that, the remote ID must be globally unique.
- **Circuit ID**
This sub-option may be added by DHCP relay agents which terminate switched or permanent circuits. It encodes an agent-local identifier of the circuit from which a DHCP client-to-server packet was received. It is intended for use by DHCP relay agents in forwarding DHCP responses back to the proper circuit.

To specify a remote ID, use the following command.

Command	Mode	Description
system-remote-id hex <i>HEXSTRING</i>	Option-82	Specifies a remote ID. (default: system MAC address)
system-remote-id ip <i>A.B.C.D</i>		
system-remote-id text <i>REMOTE-ID</i>		

To specify a circuit ID, use the following command.

Command	Mode	Description
system-circuit-id PORTS hex <i>HEXSTRING</i>	Option-82	Specifies a circuit ID. (default: port number)
system-circuit-id PORTS index <i><0-65535></i>		
system-circuit-id PORTS text <i>CIRCUIT-ID</i>		

To delete a specified remote and circuit ID, use the following command.

Command	Mode	Description
no system-remote-id	Option-82	Removes the change of form of Remote-ID or Circuit-id
no system-circuit-id PORTS		

8.8.6.3 Option-82 Reforwarding Policy

A DHCP relay agent may receive a DHCP packet from a DHCP server or another DHCP relay agent that already contains relay information. You can specify a DHCP option 82 re-forwarding policy to be suitable for the network.

To configure the policy for Option-82 packet, use the following command.

Command	Mode	Description
policy {replace keep drop}	Option-82	Configures the policy of option-82 packet: replace: replaces an existing address with option82 information of relay or server. keep: keeps an option-82 information (default). drop: drops an option-82 packet.

- **drop** means to throw away option-82 packet.
- **keep** means that relay agent transmits packets preserving option-82 which the agent sends.
- **replace** means to transmit by changing into its option-82 information.

It is possible to configure the rule for option-82 packets when the hiD 6610 S311 is DHCP relay agent. By default, the rule for Option-82 packet is configured as **keep**.

8.8.6.4 Configuring option-82 information

DHCP server decides whether IP addresses are assigned or not by identifying port number and Remote-ID included Option-82 packet. If you want to limit the number of IP address, you should configure the port number and remote-id that will be permitted to assign IP address

To configure Remote-ID and the number of IP addresses to be available for allocation, use the following command.

Command	Mode	Description
remote-id hex <i>HEXSTRING</i> lease-limit <i>NUMBER</i>	Option-82	Sets Remote ID which will be permitted to be assigned and limits the numbers of IP-address HEXSTRING: Remote-id of hexadecimal string style REMOTE-ID: Remote-id of ASCII string style A.B.C.D: Remote-id IP address NUMBER: the number of IP addresses <0-2147483637>
remote-id ip <i>A.B.C.D</i> lease-limit <i>NUMBER</i>		
remote-id text <i>REMOTE-ID</i> lease-limit <i>NUMBER</i>		

To remove above configurations, use the following command.

Command	Mode	Description
no remote-id hex <i>HEXSTRING</i> lease-limit	Option-82	Deletes Remote ID configuration and limitation of the numbers of IP-address
no remote-id ip <i>IP-ADDRESS</i> lease-limit		
no remote-id text <i>REMOTE-ID</i> lease-limit		
no remote-id all lease-limit		

Configuring Remote-ID with IP pool

Administrator is able to configure Remote-id with specified IP pool at the same time. Use the following command.

Command	Mode	Description
remote-id hex <i>HEXSTRING</i> pool <i>NAME</i>	Option-82	Sets Remote ID and IP Pool which will be permitted to be assigned IP address.
remote-id ip <i>IP-ADDRESS</i> pool <i>NAME</i>		
remote-id text <i>REMOTE-ID</i> pool <i>NAME</i>		

To remove above configurations, use the following command.

Command	Mode	Description
no remote-id hex <i>HEXSTRING</i> pool	Option-82	Deletes Remote ID and IP pool configuration
no remote-id ip <i>IP-ADDRESS</i> pool		
no remote-id text <i>REMOTE-ID</i> pool		
no remote-id all pool		

Configuring Remote-ID & Circuit-ID

After you set remote-id and circuit-id, the switch is configured to permit the packets with these remote-id and circuit-id only. To configure Remote-id and Circuit-id for limitation of the number of IP addresses, Use the following command.

Command	Mode	Description
remote-id hex <i>HEXSTRING</i> circuit-id hex <i>HEXSTRING</i> lease-limit <i>NUMBER</i>	Option-82	Sets Remote ID and circuit ID which will be permitted to be assigned and limits the numbers of IP-address HEXSTRING: Remote-id of hexadecimal string style REMOTE-ID: Remote-id of ASCII string style CIRCUIT-ID: Circuit-id of ASCII string style. A.B.C.D: Remote-id IP address NUMBER: the number of IP addresses <0-2147483637> 0-65535 : Circuit-id of numeric style
remote-id hex <i>HEXSTRING</i> circuit-id index <0-65535> lease-limit <i>NUMBER</i>		
remote-id hex <i>HEXSTRING</i> circuit-id text <i>CIRCUIT-ID</i> lease-limit <i>NUMBER</i>		
remote-id ip <i>A.B.C.D</i> circuit-id hex <i>HEXSTRING</i> lease-limit <i>NUMBER</i>		
remote-id ip <i>A.B.C.D</i> circuit-id index <0-65535> lease-limit <i>NUMBER</i>		
remote-id ip <i>A.B.C.D</i> circuit-id text <i>CIRCUIT-ID</i> lease-limit <i>NUMBER</i>		
remote-id text <i>REMOTE-ID</i> circuit-id hex <i>HEXSTRING</i> lease-limit <i>NUMBER</i>		
remote-id text <i>REMOTE-ID</i> circuit-id index <0-65535> lease-limit <i>NUMBER</i>		
remote-id text <i>REMOTE-ID</i> circuit-id text <i>CIRCUIT-ID</i> lease-limit <i>NUMBER</i>		

To delete the configuration of remote-id and circuit-id for IP address limit, use the following command.

Command	Mode	Description
no remote-id hex <i>HEXSTRING</i> circuit-id hex <i>HEXSTRING</i> lease-limit	Option-82	Deletes Remote ID and Circuit ID which to be assigned and limits the numbers of IP-address REMOTE-ID:IP-address or Mac-address NUMBER: the number of IP addresses <0-2147483637>
no remote-id hex <i>HEXSTRING</i> circuit-id index <0-65535> lease-limit		
no remote-id hex <i>HEXSTRING</i> circuit-id text <i>CIRCUIT-ID</i> lease-limit		
no remote-id hex <i>HEXSTRING</i> circuit-id all lease-limit		
no remote-id ip <i>A.B.C.D</i> circuit-id hex <i>HEXSTRING</i> lease-limit		
no remote-id ip <i>A.B.C.D</i> circuit-id index <0-65535> lease-limit		
no remote-id ip <i>A.B.C.D</i> circuit-id text <i>CIRCUIT-ID</i> lease-limit		
no remote-id ip <i>A.B.C.D</i> circuit-id all lease-limit		
no remote-id text <i>REMOTE-ID</i> circuit-id hex <i>HEXSTRING</i> lease-limit		
no remote-id text <i>REMOTE-ID</i> circuit-id index <0-65535> lease-limit		
no remote-id text <i>REMOTE-ID</i> circuit-id text <i>CIRCUIT-ID</i> lease-limit		
no remote-id text <i>REMOTE-ID</i> circuit-id all lease-limit		

To configure Remote-id and circuit-id with specified IP pool at the same time. Use the following command.

Command	Mode	Description
remote-id hex <i>HEXSTRING</i> circuit-id hex <i>HEXSTRING</i> pool NAME	Option-82	Sets Remote ID and circuit ID with specified IP Pool which will be permitted to be assigned IP address HEXSTRING: Remote-id of hexadecimal string style REMOTE-ID: Remote-id of ASCII string style CIRCUIT-ID: Circuit-id of ASCII string style. A.B.C.D: Remote-id IP address NUMBER: the number of IP addresses <0-2147483637> 0-65535 : Circuit-id of numeric style- NAME: enters the pool name
remote-id hex <i>HEXSTRING</i> circuit-id index <0-65535> pool NAME		
remote-id hex <i>HEXSTRING</i> circuit-id text <i>CIRCUIT-ID</i> pool NAME		
remote-id ip <i>A.B.C.D</i> circuit-id hex <i>HEXSTRING</i> pool NAME		
remote-id ip <i>A.B.C.D</i> circuit-id index <0-65535> pool NAME		
remote-id ip <i>A.B.C.D</i> circuit-id text <i>CIRCUIT-ID</i> pool NAME		
remote-id text <i>REMOTE-ID</i> circuit-id hex <i>HEXSTRING</i> pool NAME		
remote-id text <i>REMOTE-ID</i> circuit-id index <0-65535> pool NAME		
remote-id text <i>REMOTE-ID</i> circuit-id text <i>CIRCUIT-ID</i> pool NAME		

To delete the configuration of remote-id and circuit-id with specified DHCP pool, use the following command.

Command	Mode	Description
no remote-id hex <i>HEXSTRING</i> circuit-id hex <i>HEXSTRING</i> pool	Option-82	Deletes Remote ID and Circuit ID which will be permitted to be assigned IP address
no remote-id hex <i>HEXSTRING</i> circuit-id index <0-65535> pool		
no remote-id hex <i>HEXSTRING</i> circuit-id text <i>CIRCUIT-ID</i> pool		
no remote-id hex <i>HEXSTRING</i> circuit-id all pool		
no remote-id ip <i>A.B.C.D</i> circuit-id hex <i>HEXSTRING</i> pool		
no remote-id ip <i>A.B.C.D</i> circuit-id index <0-65535> pool		
no remote-id ip <i>A.B.C.D</i> circuit-id text <i>CIRCUIT-ID</i> pool		
no remote-id ip <i>A.B.C.D</i> circuit-id all pool		
no remote-id text <i>REMOTE-ID</i> circuit-id hex <i>HEXSTRING</i> pool		
no remote-id text <i>REMOTE-ID</i> circuit-id index <0-65535> pool		
no remote-id text <i>REMOTE-ID</i> circuit-id text <i>CIRCUIT-ID</i> pool		
no remote-id text <i>REMOTE-ID</i> circuit-id all pool		

8.8.6.5 Option-82 Trust Policy

This feature prevents to be exhausted DHCP pool's IP addresses from DHCP packet with unexpected option-82 field information. After issuing the **trust default deny** command, you can control which option-82 field information is valid or not.

Default Trust Policy

To configure the default trust policy, use the following command.

Command	Mode	Description
trust default {deny permit}	Option82	Configures DHCP Option82 Trust function.

Trust Policy for Remote ID

To configure the trust option82, use the following command.

Command	Mode	Description
trust remote-id hex <i>HEXSTRING</i>	Option82	Changes the type of remote-id of a trust option82.
trust remote-id ip <i>IP-ADDRESS</i>		
trust remote-id text <i>REMOTE-ID</i>		
no trust remote-id hex <i>HEXSTRING</i>		Disables DHCP Option82 Trust function.
no trust remote-id ip <i>IP-ADDRESS</i>		
no trust remote-id text <i>REMOTE-ID</i>		

Trust Policy for Physical Port

To specify a trust policy for physical port, use the following command.

Command	Mode	Description
trust port <i>PORTS</i>	Option82	Specifies a trust policy for physical ports.
no trust port { <i>all</i> <i>PORTS</i> }		Disables DHCP Option82 Trust function.

8.8.6.6 Simplified DHCP Option 82 in Layer 2

Usually, DHCP relay is used in Layer 3 network. But in Layer 2 network, if you want to configure DHCP relay with option 82, use the simplified option 82.

In case of a DHCP option 82 environment, when forwarding DHCP messages to a DHCP server, a DHCP relay agent normally adds a relay agent information option to the DHCP messages and replaces a gateway address in the DHCP messages with a relay agent address.

On the other hand, in case of a simplified DHCP option 82 environment, a DHCP relay agent adds a relay agent information option to the DHCP messages without replacement of a gateway address field in the DHCP messages. This allows an enhanced security and efficient IP assignment in the Layer 2 environment with a relay agent information option.

To enable and disable the simplified option82, use the following command.

Command	Mode	Description
ip dhcp active simplified-option82	Global	Enables a simplified DHCP option 82.
no ip dhcp active simplified-option82		Disables a simplified DHCP option 82.



To enable DHCP Option 82 function in Layer 2 network, DHCP server or DHCP relay agent should be disabled previously in the system.

8.8.7 DHCP Client

The interfaces of the hiD 6610 S311 can be assigned IP addresses from DHCP server dynamically. If the hiD 6610 S311 is configured as DHCP client itself, it works as transparent switch in Layer 2 network. However, the switch can't be configured as DHCP server and DHCP relay agent in DHCP client environment.

8.8.7.1 Enabling DHCP Client (Required)

To request an IP address on an interface from a DHCP server, use the following command. This command allows the interface to receive its IP address. Use the following command on *Interface configuration* mode.

Command	Mode	Description
ip address dhcp	Interface	Enables a DHCP client on an interface
no ip address dhcp		Disables a DHCP client

8.8.7.2 DHCP Client ID

To specify a client ID, use the following command.

Command	Mode	Description
ip dhcp client client-id hex <i>HEXSTRING</i>	Interface	Specifies a client ID. CLIENT-ID: client-id of ASCII string type HEXSTRING: client-id of HEX string type
ip dhcp client client-id ascii <i>CLIENT-ID</i>		

To remove the configuration, use the following command.

Command	Mode	Description
no ip dhcp client client-id	Interface	Removes a client ID of DHCP client

8.8.7.3 DHCP Class ID

The class identifier depends on vendors to specify the type of device that is requesting an IP address.

To specify the class identifier, use the following command.

Command	Mode	Description
ip dhcp client class-id hex <i>HEX-STRING</i>	Interface	Specifies a class ID of the client.
ip dhcp client class-id text <i>STRING</i>		

To remove the configuration, use the following command.

Command	Mode	Description
no ip dhcp client class-id	Interface	Removes the class ID of the client.

8.8.7.4 Lease Time of Client

To specify IP lease time that is requested to a DHCP server, use the following command.

Command	Mode	Description
ip dhcp client lease <120-2147483637>	Interface	Specifies IP lease time in the unit of second (default: 3600).
no ip dhcp client lease		Deletes a specified IP lease time.

8.8.7.5 Forcing a Release or Renewal of DHCP Client

The DHCP release and renew commands support two independent operation: immediate release a DHCP lease for a DHCP client and force DHCP renewal of a lease for a DHCP client.

To force a release of a DHCP release for a DHCP client, use the following command.

Command	Mode	Description
release dhcp <i>INTERFACE</i>	Enable	Forces a release of a DHCP lease. <i>INTERFACE</i> : enters specified Interface name.

To force a renewal of a DHCP release for a DHCP client, use the following command.

Command	Mode	Description
renew dhcp <i>INTERFACE</i>	Enable	Forces a renewal of a DHCP lease. <i>INTERFACE</i> : enters specified Interface name.

8.8.7.6 Displaying DHCP Client Configuration

To display a DHCP client configuration, use the following command.

Command	Mode	Description
show ip dhcp client <i>INTERFACE</i>	Enable Global Interface	Shows a configuration of DHCP client.

8.8.8 DHCP Snooping

The hiD 6610 S311 switch offers an DHCP security feature, called DHCP snooping that allows network administrator to be able to utilize and configure the certain ports to restrict access of only authorized traffic.

Enabling DHCP snooping on a port will only permit authorized traffic and filter out all other traffics, which are not recorded in DHCP snooping table. For instance, once a user gets

DHCP address from the server, his IP address, MAC address and Lease Time are stored in the DHCP snooping table. Only this IP address traffic is permitted and all other users who have static IP address or don't have dynamic assigned IP address will be denied.

This feature is designed for isolating malicious activity and disallowing possible attacks from unauthorized users.

8.8.8.1 Enabling DHCP Snooping

To enable DHCP snooping globally, use the following command

Command	Mode	Description
ip dhcp snooping	Global	Enables the DHCP snooping on the system.
no ip dhcp snooping		Disables the DHCP snooping on the system. (default)

8.8.8.2 DHCP snooping on port

To assign the port of DHCP Snooping function, use the following command.

Command	Mode	Description
ip dhcp verify source port <i>PORTS</i>	Global	Configures DHCP snooping function to specified port. PORTS: enters port number
no ip dhcp verify source port <i>PORTS</i>		Removes DHCP function from specified port

8.8.8.3 DHCP Rate Limit on Layer 2

Limit Rate

To set the number of DHCP packet per second (pps) that an interface can receive, use the following command.

Command	Mode	Description
ip dhcp snooping limit-rate <i>PORTS</i> <1-255>	Global	Sets a rate limit for DHCP packets.
no ip dhcp snooping limit-rate <i>PORTS</i>		Deletes a rate limit for DHCP packets.



Normally, the DHCP rate limit is specified to untrusted interfaces and 15 pps is recommended for a proper value. However, if you want to set a rate limit for trusted interfaces, keep in mind that trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit to a higher value.

8.8.8.4 Displaying DHCP Snooping Configuration

The DHCP snooping table contains IP address, MAC address and Lease Time that correspond to the authorized IP address.

To display DHCP snooping table, use the following command.

Command	Mode	Description
show ip dhcp snoop [PORTS]	Global	Shows DHCP Snooping table.

To remove specific IP address from the DHCP Snooping table, use the following command.

Command	Mode	Description
clear ip dhcp snooping PORTS ADDRESS/M	Enable Global	Deletes IP address on DHCP Snooping table. A.B.C.D/M: IP address of DHCP snoop entry

8.8.9 Displaying DHCP Statistics and Configuration

In the hiD 6610 S311, user can verify and delete DHCP packet statistics that transmitted to other switches with below command.

Command	Mode	Description
show ip dhcp statistics	Enable	Shows DHCP packet statistics.
clear ip dhcp statistics	Global Bridge	Deletes DHCP packet statistics information.

8.8.10 Lease Database Back-up & Reset

For the hiD 6610 S311, it is possible to save DHCP lease database. To back up DHCP lease database, use the following command.

Command	Mode	Description
ip dhcp leasedb backup IP- ADDRESS <1-2147483637>	Global	Backs up DHCP lease database and configure the interval. 1-2147483637: Interval time for back (Unit is second)
no ip dhcp leasedb backup		Deletes Back up lease database

To reset the DHCP lease database, use the following commands.

Command	Mode	Description
clear ip dhcp leasedb IP-ADDRESS/M	Enable	Resets a DHCP lease database per subnet.
clear ip dhcp leasedb pool POOL-NAME	Global	Resets a DHCP lease database per IP pool.
clear ip dhcp leasedb all	Bridge	Resets entire DHCP lease database.

8.8.11 DHCP Filtering

8.8.11.1 DHCP Packet Filtering

For the hiD 6610, it is possible to block the specific client with MAC address. If the blocked MAC address by administrator requests IP address, the server does not assign IP. This function is to strength the security of DHCP server.

The following is the function of blocking to assign IP address on a port.

Command	Mode	Description
ip dhcp filter-port <i>PORTS</i>	Global	Configures a port in order not to assign IP.
no ip dhcp filter-port <i>PORTS</i>		Disables DHCP packet filtering.

The following is to designate MAC address which IP address is not assigned.

Command	Mode	Description
ip dhcp filter-address <i>MAC-ADDRESS</i>	Global	Blocks a MAC address in case of requesting IP address.
no ip dhcp filter-address <i>MAC-ADDRESS</i>		Disables DHCP MAC filtering.

8.8.11.2 DHCP Server Packet Filtering

DHCP (Dynamic Host Configuration Protocol) makes DHCP server assign IP address to DHCP clients automatically and manage the IP address. Most ISP operators provide the service as such a way. At this time, if a DHCP client connects with the equipment that can be the other DHCP server such as Internet access gateway router, communication failure might be occurred.

DHCP filtering helps to operate DHCP service by blocking DHCP REQUEST which enters through subscriber's port and goes out into uplink port or the other subscriber's port and DHCP REPLY which enters to the subscriber's port.

In the Fig. 8.34, server A has the IP area from 192.168.10.1 to 192.168.10.10. Suppose a user connects with client 3 that can be DHCP server to A in order to share IP address from 10.1.1.1 to 10.1.1.10.

Here, if client 1 and client 2 are not blocked from client 3 of DHCP server, client 1 and client 2 will request and receive IP from client 3 so that communication blockage will be occurred. Therefore, the filtering function should be configured between client 1 and client 3, client 2 and client 3 in order to make client 1 and client 2 receive IP without difficulty from DHCP server A.

To enable the DHCP server packet filtering, use the following command.

Command	Mode	Description
dhcp-server-filter <i>PORTS</i>	Bridge	Enables the DHCP server packet filtering.
no dhcp-server-filter <i>PORTS</i>		Disables the DHCP server packet filtering.

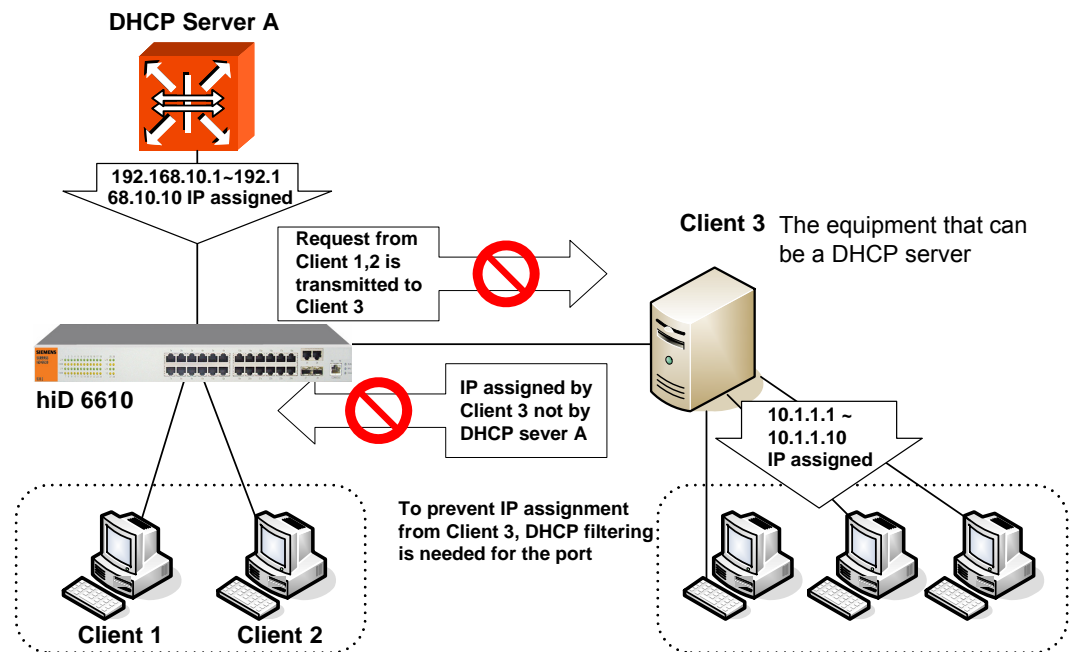


Fig. 8.34 DHCP Server Packet Filtering

To see DHCP server filtering status, use the following command.

Command	Mode	Description
show dhcp-server filter	Enable Global	Displays the status of DHCP server filtering of all ports.

8.8.12 Debugging DHCP

To enable and disable the debugging DHCP, use the following command.

Command	Mode	Description
debug dhcp {filter lease packet service all}	Enable	Enables a debugging DHCP.
no debug dhcp {filter lease packet service all}		Disables a debugging DHCP.

8.9 Ethernet Ring Protection (ERP)

The ERP is a Siemens protection protocol and procedure to protect Ethernet ring topologies. It is a fast failure detection and recovery so that it decreases the time to prevent Loop under 50ms.

The main characteristics of the ERP are the follows:

- It required no additional underlying protection mechanism within the ring configuration, the complete functionality is implemented on the interface units of the system and does not require additional dedicated hardware which may raise network complexity and costs.
- It is a unique robustness functionality which runs on every network element involved in the ring configurations. It means each system is active part of the ring protection mechanism. Therefore, it guarantees a maximum of 50 ms to switch over towards a new configuration after link or system failures.
- ERP and STP cannot be configured at once.

8.9.1 ERP Operation

Ethernet Ring Protection (ERP) is a concept and protocol optimized for fast failure detection and recovery on Ethernet ring topologies. The Protection of fast failure detection and recovery occurs on RM Node. An Ethernet ring consists of two or more switches. One of the nodes on the ring is designated as redundancy manager (RM) and the two ring ports on the RM node are configured as primary port and secondary port respectively.

The RM blocks the secondary port for all non-control traffic belongs to this ERP domain. Here, if Line failure occurs, the Nodes detecting Link Failure transmit Link Down message and Link Failure port becomes Blocking status. When the RM nodes receive this link-down message, it immediately declares failed state, and opens the logically blocked protected VLANs on the secondary port. Then, Ethernet Ring restarts the communication.

The following is ERP operation when Link Failure occurs.

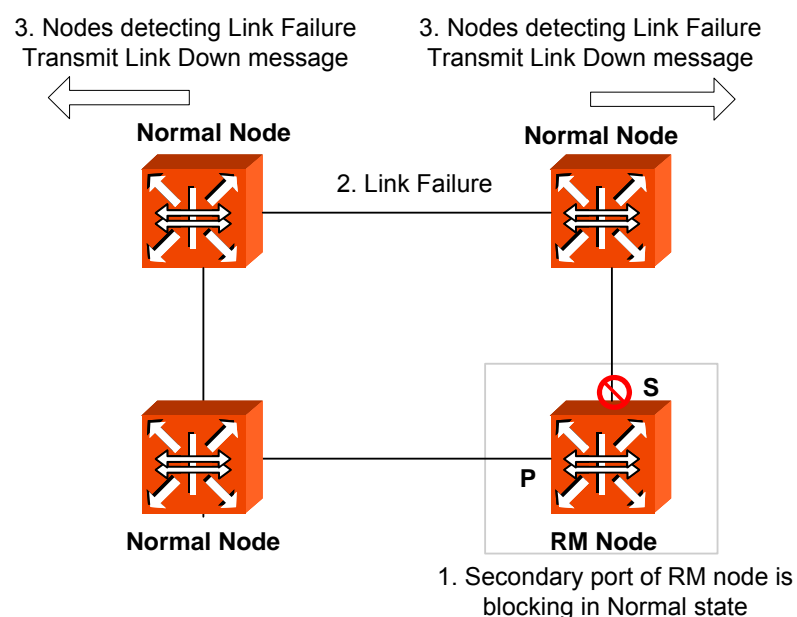


Fig. 8.35 Ethernet Ring Protocol Operation in Failure State

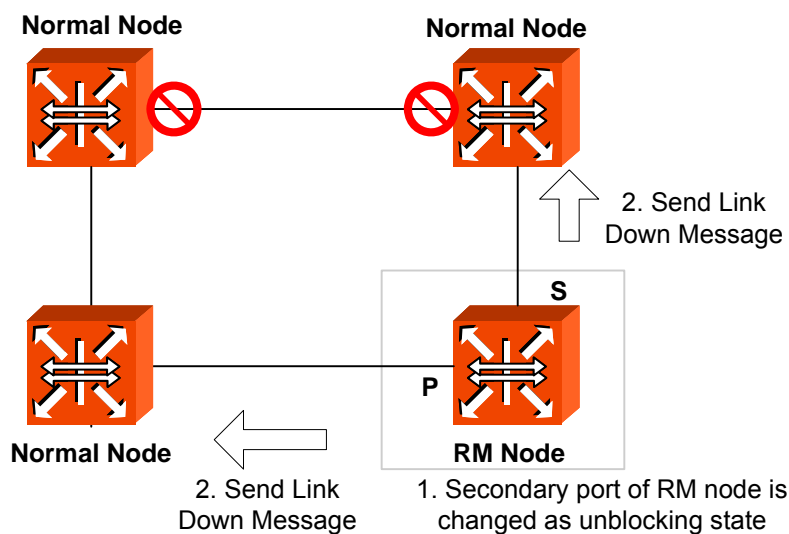


Fig. 8.36 Ring Protection

When a Link Failure is recovered, a temporary loop may occur. To rectify this condition, ERP sends a “link up” message to the RM. The RM will logically block the protected VLANs on its secondary port and generate a “RM link up” packet to make sure that all transit nodes are properly reconfigured. This completes fault restoration and the ring is back in normal state.

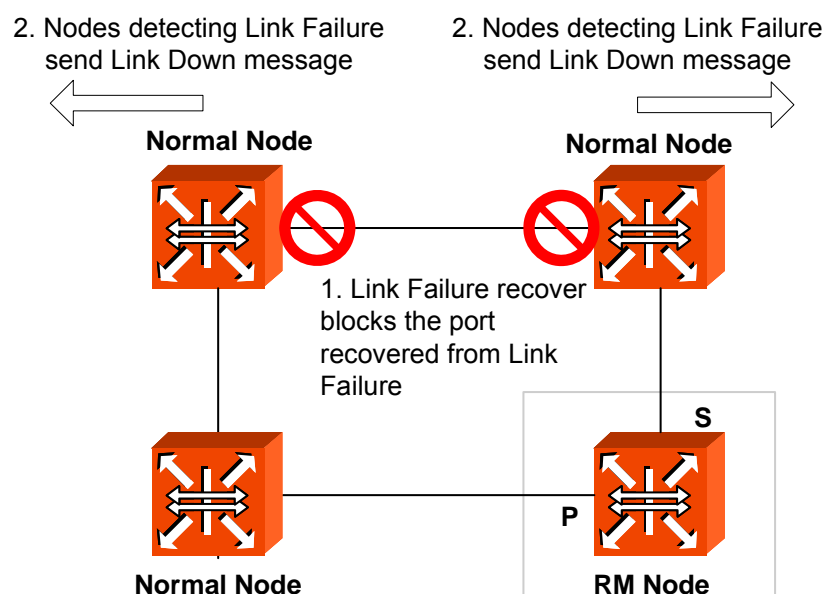


Fig. 8.37 Link Failure Recovery

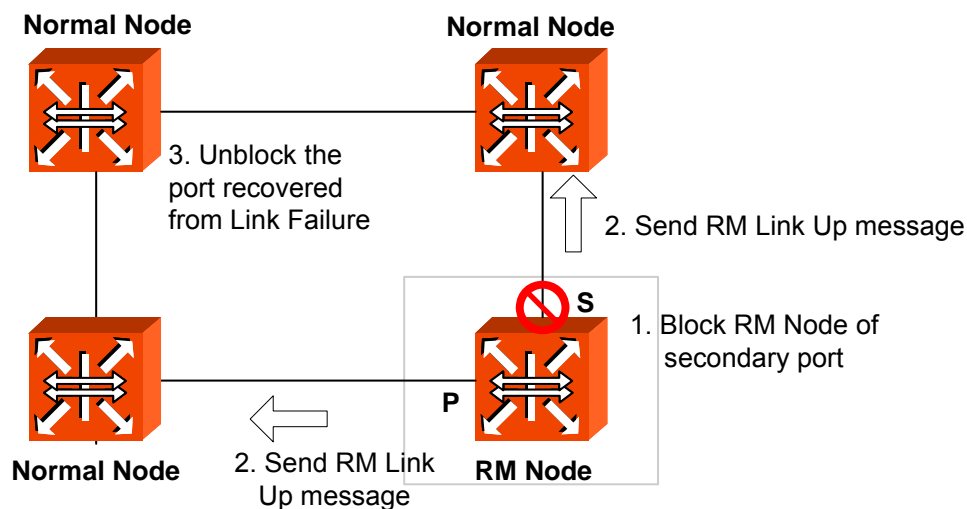


Fig. 8.38 Ring Recovery

8.9.2 Loss of Test Packet (LOTP)

ERP recognizes the Link Failure using Loss of Test Packet (LOTP). RM Node regularly sends RM Test Packet message. If the message is not retransmitted to RM Node through Ethernet Ring, it means that Loop doesn't occur. Therefore, RM Node unblocks Secondary port. The condition that RM Test Packet from RM Node doesn't return is LOTP state.

On the other hand, if RM Test Packet is retransmitted to RM Node through Ethernet Ring, Loop may occur. In this condition, RM Node blocks Secondary port.

8.9.3 Configuring ERP

8.9.3.1 ERP Domain

To realize ERP, you should first configure domain for ERP. To configure the domain, use the following command.

Command	Mode	Description
erp domain <i>DOMAIN-ID</i>	Bridge	Creates ERP domain. DOMAIN-ID: control VLAN ID of domain <1-4094>
no erp domain { all <i>DOMAIN-ID</i> }		Deletes ERP domain.

To specify a description for configured domain, use the following command.

Command	Mode	Description
erp description <i>DOMAIN-ID</i> <i>DESCRIPTION</i>	Bridge	Specifies a description of domain.

8.9.3.2 RM Node

To configure RM Node, use the following command.

Command	Mode	Description
erp rmnode <i>DOMAIN-ID</i>	Bridge	Configures RM node of ERP node mode.
no erp rmnode <i>DOMAIN-ID</i>		Configures ERP node mode as normal node.

8.9.3.3 Port of ERP domain

To configure Primary Port and Secondary port of RM Node, use the following command.

Command	Mode	Description
erp port <i>DOMAIN-ID</i> primary <i>PORT secondary PORT</i>	Bridge	Configures ports of ERP domain



Primary port and secondary port should be different.

8.9.3.4 Protected VLAN

To configure Protected VLAN of ERP domain, use the following command.

Command	Mode	Description
erp protections <i>DOMAIN-ID VID</i>	Bridge	Configures protected VLAN of ERP domain VID: VLAN ID

To delete the configured Protected VLAN, use the following command.

Command	Mode	Description
no erp protections <i>VID</i>	Bridge	Deletes protected VLAN of ERP domain. VID: VLAN ID

8.9.3.5 Protected Activation

To configure ERP Protected Activation, use the following command.

Command	Mode	Description
erp activation <i>DOMAIN-ID</i>	Bridge	Configures ERP Protected Activation.

To disable ERP Protected Activation, use the following command

Command	Mode	Description
no erp activation <i>DOMAIN-ID</i>	Bridge	Disables ERP Protected Activation.

8.9.3.6 Manual Switch to Secondary

To configure Manual Switch to Secondary, use the following command.

Command	Mode	Description
erp ms-s <i>DOMAIN-ID</i>	Bridge	Configures ERP manual switch to secondary

To disable Manual Switch to Secondary, use the following command.

Command	Mode	Description
no erp ms-s <i>DOMAIN-ID</i>	Bridge	Disables ERP manual switch to secondary

8.9.3.7 Wait-to-Restore Time

To configure Wait-to-Restore Time, use the following command.

Command	Mode	Description
erp wait-to-restore <i>DOMAIN-ID</i> <i><1-720></i>	Bridge	Configures ERP wait-to-restore time 1-720: Wait to restore time in second

To return the configured Wait-to-Restore Time as Default, use the following command.

Command	Mode	Description
no erp wait-to-restore <i>DOMAIN-ID</i>	Bridge	Configures ERP wait-to-restore time as default value

8.9.3.8 Learning Disable Time

To configure ERP Learning Disable Time, use the following command.

Command	Mode	Description
erp learn-dis-time <i>DOMAIN-ID</i> <i><0-500></i>	Bridge	Configures ERP learning disable time 0-500: learning disabling time (unit: millisecond)

To return the configured Learning Disable Time as Default, use the following command.

Command	Mode	Description
no erp learn-dis-time <i>DOMAIN-ID</i>	Bridge	Configures ERP learning disable time as default value

8.9.3.9 Test Packet Interval

To configure ERP Test Packet Interval, use the following command.

Command	Mode	Description
erp test-packet-interval <i>DO-MAIN-ID</i> <i><10-500></i>	Bridge	Configures ERP test packet interval 10-500: packet interval (unit: millisecond)

To return ERP Test Packet Interval as Default, use the following command.

Command	Mode	Description
no erp test-packet-interval <i>DO-MAIN-ID</i>	Bridge	Configures ERP test packet interval as default value

8.9.3.10 Displaying ERP Configuration

To display a configuration for ERP, use the following command.

Command	Mode	Description
show erp {all <i>DOMAIN-ID</i> }	Enable Global Bridge	Shows the information of ERP

8.10 Stacking

It is possible to manage several switches with one IP address by using stacking. If there's a limitation for using IP addresses and there are too many switches which you must manage, you can manage a number of switches with a IP address using this stacking function.

Switch stacking technology available in the industry today provides two main benefits to customers. The first benefit is the ability to manage a group of switches using a single IP address. The second benefit is the ability to interconnect two or more switches to create a distributed fabric, which behaves in the network as a unified system. The hiD 6610 S311 provides the stacking technology's benefits for the customer.



It is possible to configure stacking function for switches from 2 to 16.

The following is an example of the network where stacking is configured.

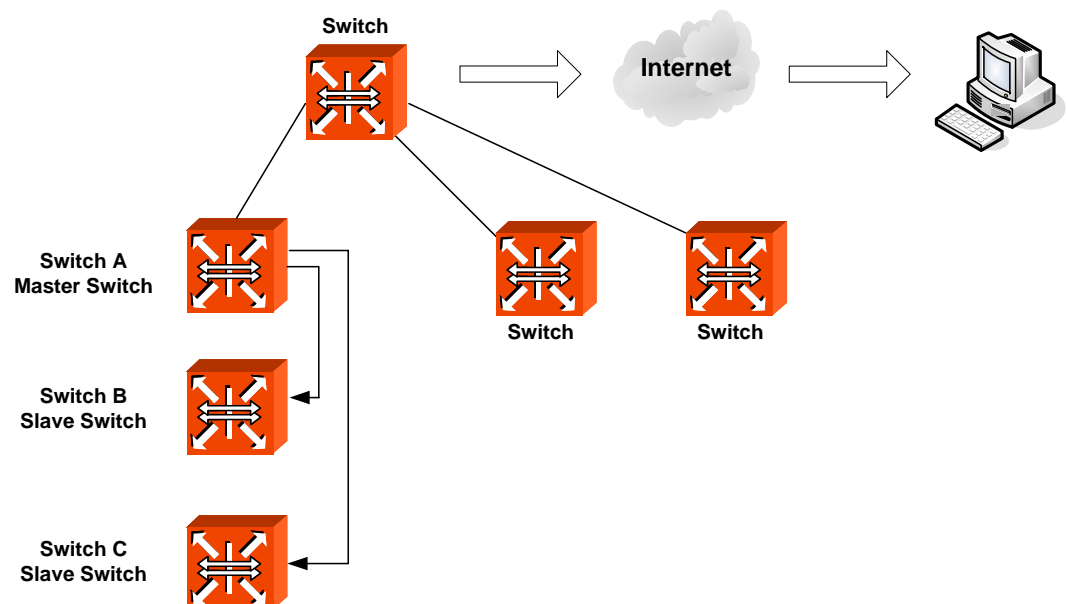


Fig. 8.39 Example of Stacking

A switch, which is supposed to manage the other switches in stacking is named as Master switch and the other switches managed by Master switch are named as Slave switch. Regardless of installed place or connection state, Master switch can check and manage all Slave switches.

The below steps are provided to configure stacking.

8.10.1 Switch Group

You should configure all the switches configured with stacking function to be in the same VLAN. To configure the switches as a switch group belongs in the same VLAN, use the following command.

Command	Mode	Description
stack device <i>NAME</i>	Global	Configures device name or VID



For managing the stacking function, the port connecting Master switch and Slave switch must be in the same VLAN.

8.10.2 Designating Master and Slave Switch

Designate Mater switch using the following command.

Command	Mode	Description
stack master	Global	Designates Master switch

After designating Master switch, register Slave switch for Master switch. To register Slave switch or delete the registered Slave switch, use the following command.

Command	Mode	Description
stack add <i>MACADDR</i> [<i>DE-SCRIPTON</i>]	Global	Registers slave switch. MACADDR: MAC address
stack del <i>MACADDR</i>		Deletes slave switch.



To make stacking operate well, it is required to enable the interface of Slave switch. The switches in different VLANs can not be added to the same switch group.

You should designate Slave switch registered in Master Switch as Slave Switch. To designate Slave switch, use the following command.

Command	Mode	Description
stack slave	Global	Designates as a slave switch

8.10.3 Disabling Stacking

To disable stacking, use the following command.

Command	Mode	Description
no stack	Global	Disables the stacking function

8.10.4 Displaying Stacking Status

Command	Mode	Description
show stack	Enable Global	Shows a configuration of stacking

8.10.5 Accessing to Slave Switch from Master Switch

After configuring all stacking configurations, it is possible to configure and manage by accessing to Slave switch from Master switch.

To access to Slave switch from Master switch, use the following command in Bridge configuration mode.

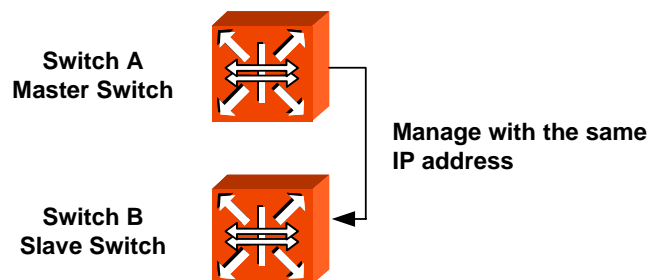
Command	Mode	Description
rcommand <i>NODE</i>	Global	Accesses to a slave switch. NODE: node number

NODE means node ID from configuring stacking in Slave switch. If you input the above command in Master switch, Telnet connected to Slave switch is displayed and it is possible to configure Slave switch using DSH command. If you use the exit command in Telnet, the connection to Slave switch is down.

8.10.6 Sample Configuration

[Sample Configuration 1] Configuring Stacking

The following is a stacking configuration by designating SWITCH A as a master and SWITCH B as a slave.



Step 1

Assign IP address in Interface configuration mode of Switch and enable interface using “no shutdown” command. In order to enter into *Interface configuration* mode, you should open *Interface configuration* mode of VLAN to register as a switch group for stacking.

The following is an example of configuring Interface of switch group as 1.

```
SWITCH_A# configure terminal
SWITCH_A(config)# interface 1
SWITCH_A(interface)# ip address 192.168.10.1/16
SWITCH_A(interface)# no shutdown
SWITCH_A(interface)#
```



If there are several switches, rest of them are managed by a single IP address of Master switch. Therefore you don't need to configure IP address in Slave switch.

Step 2

Configure Switch A as Master switch. Configure VLAN to belong in the same switch group after registering Slave switch, configure it as a Master switch.

<Switch A – Master Switch>

```
SWITCH_A(config)# stack master
SWITCH_A(config)# stack device default
SWITCH_A(config)# stack add 00:d0:cb:22:00:11
```

Step 3

Configure VLAN in order to belong to the same switch group in Switch B registered by Master switch as Slave switch and configure as a Slave switch.

<Switch B – Slave Switch>

```
SWITCH_B(config)# stack slave
SWITCH_B(config)# stack device default
```

Step 4

Check the configuration. The information you can check in Master switch and Slave switch is different as below.

<Switch A – Master Switch>

```
SWITCH_A(config)# show stack
device : default
node ID : 1
node  MAC address      status  type          name          port
  1   00:d0:cb:0a:00:aa  active  SURPASS hiD 6610 S311 SWITCH_A    24
  2   00:d0:cb:22:00:11  active  SURPASS hiD 6610 S311 SWITCH_B    24
SWITCH_A(config)#
```

<Switch B – Slave Switch>

```
SWITCH_B(config)# show stack
device : default
node ID : 2
SWITCH_B(config)#
```

[Sample Configuration 2] Accessing from Master Switch to Slave Switch

The following is an example of accessing to Slave switch from Master switch configured in [Sample Configuration 1]. If you show the configuration of Slave switch in [Sample Configuration 1], you can recognize node-number is 2.

```
SWITCH(bridge)# rcommand 2
Trying 127.1.0.1(23)...
Connected to 127.1.0.1.
Escape character is '^]'.
SWITCH login: admin
Password:
SWITCH#
```

To disconnect, input as below.

```
SWITCH# exit
Connection closed by foreign host.
SWITCH(bridge)#
```

8.11 Broadcast Storm Control

The hiD 6610 S311 supports broadcast storm control for broadcast packets. Broadcast storm is overloading situation of broadcast packets since they need major part of transmit capacity. Broadcast storm may be often occurred because of difference of versions. For example, when there are mixed 4.3 BSD and 4.2 BSD, or mixed AppleTalk Phase I and Phase II in TCP/IP, Storm may occur

In addition, when information of routing protocol regularly transmitted from router incorrectly recognized by system, which does not support the protocol, Broadcast Storm may be occurred.

Broadcast Storm Control is operated by system counts how many Broadcast packets are there for a second and if there are packets over configured limit, they are discarded.

The hiD 6610 S311 provides not only broadcast storm but also control of multicast and DLF (Destination Lookup Fail) storm. In order to use control of multicast and DLF storm, use the following commands. Then all configurations of Broadcast storm control will be equally applied to all VLANs.

To enable multicast storm control and DLF storm control, use the following command.

Command	Mode	Description
storm-control {broadcast multicast dlf} RATE [PORTS]	Bridge	Enables broadcast, multicast, or DLF storm control respectively in a port with a user defined rate. Rate value is from 1 to 262142 for FE, and from 1 to 2097150 for GE



By default, DLF storm control is enabled and multicast storm control is disabled.

To disable multicast storm control and DLF storm control, use the following commands

Command	Mode	Description
no storm-control {broadcast multicast dlf} [PORTS]	Bridge	Disables broadcast, multicast, or DLF storm control respectively.

To display a configuration of storm control, use the following command.

Command	Mode	Description
show storm-control	Enable Global Bridge	Displays storm control configuration.

8.12 Jumbo-frame Capacity

The packet range that can be capable to accept is from 64 bytes to 1518 bytes. Therefore, packets not between these ranges will not be taken. However, the hiD 6610 S311 can accept Jumbo-frame larger than 1518 bytes through user's configuration.

To configure to accept Jumbo-frame larger than 1518 bytes, use the following command.

Command	Mode	Description
jumbo-frame <i>PORTS</i> <1518-9000>	Bridge	Configures to accept jumbo-frame between specified ranges. 1518-9000: Max packet length

To disable configuration to accept Jumbo-frame, use the following command.

Command	Mode	Description
no jumbo-frame <i>PORTS</i>	Bridge	Disables configuration to accept jumbo-frame on specified port.

To display the configuration of Jumbo-frame, use the following command.

Command	Mode	Description
show jumbo-frame	Enable Global Bridge	Shows a configuration of jumbo frame.

Sample Configuration

The following is an example of configuration to accept Jumbo-frame under 2200 bytes in port 1~10.

```
SWITCH# configure terminal
SWITCH(config)# bridge
SWITCH(bridge)# jumbo-frame 1-10 2200
SWITCH(bridge)# show jumbo-frame
    Name : Current/Default
port01 :   2200/   1518
port02 :   2200/   1518
port03 :   2200/   1518
port04 :   2200/   1518
port05 :   2200/   1518
port06 :   2200/   1518
port07 :   2200/   1518
port08 :   2200/   1518
port09 :   2200/   1518
port10 :   2200/   1518
port11 :   1518/   1518
port12 :   1518/   1518
port13 :   1518/   1518
port14 :   1518/   1518
port15 :   1518/   1518
```

```
port16 : 1518/ 1518
port17 : 1518/ 1518
(Skipped)
SWITCH(bridge)#
```

8.13 Maximum Transmission Unit (MTU)

Maximum value for the length of the data payload can be transmitted. User can control Maximum Transmission Unit (MTU) with below command.

Command	Mode	Description
mtu <64-17940>	Interface	Configures maximum MTU size.
no mtu		Returns to the default MTU size.

The following is an example of configuration to mtu size as 100.

```
SWITCH(config-if)# mtu 100
SWITCH(config-if)# show running-config interface 1
!
interface default
mtu 100
bandwidth 1m
ip address 10.27.41.181/24
SWITCH(config-if)
```

9 IP Multicast

Traditional IP network provided unicast transmission a host to send packets to a single host or broadcast transmission. However, multicast provides group transmission a host to send packets to a group of all hosts. In the multicast environment, multicast packets are delivered to a group by duplicating multicast packets.

Multicasting is divided into Layer 3 multicast routing and Layer 2 IGMP snooping. The hiD 6610 S311 supports PIM-SM/SSM of multicast routing, and V1, V2 and V3 of IGMP snooping.

Fig. 9.1 shows the example of IGMP snooping configuration network. In Layer 2 network, the hiD 6610 S311 is configured only for IGMP Snooping.

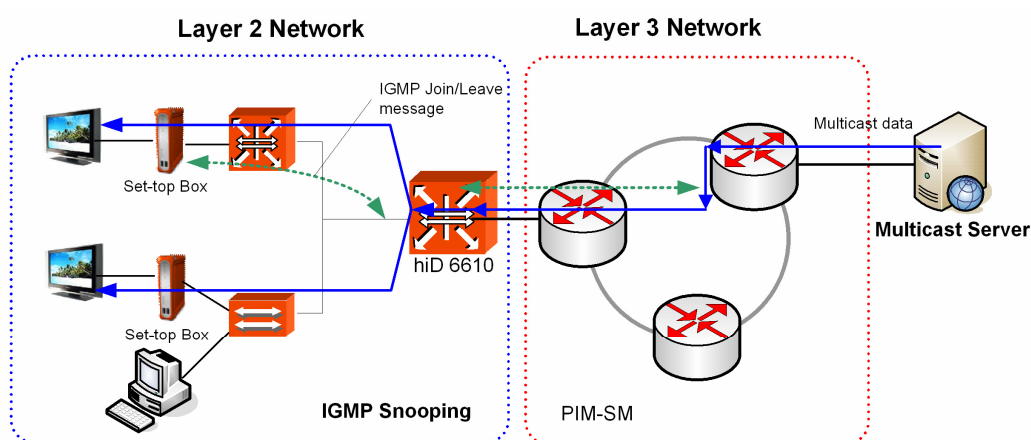


Fig. 9.1 IGMP Snooping Configuration Network

If the hiD 6610 S311 is within Layer 3 network, PIM-SM should be configured. Below the hiD 6610 S311, there is a switch that performs IGMP snooping function for subscribers.

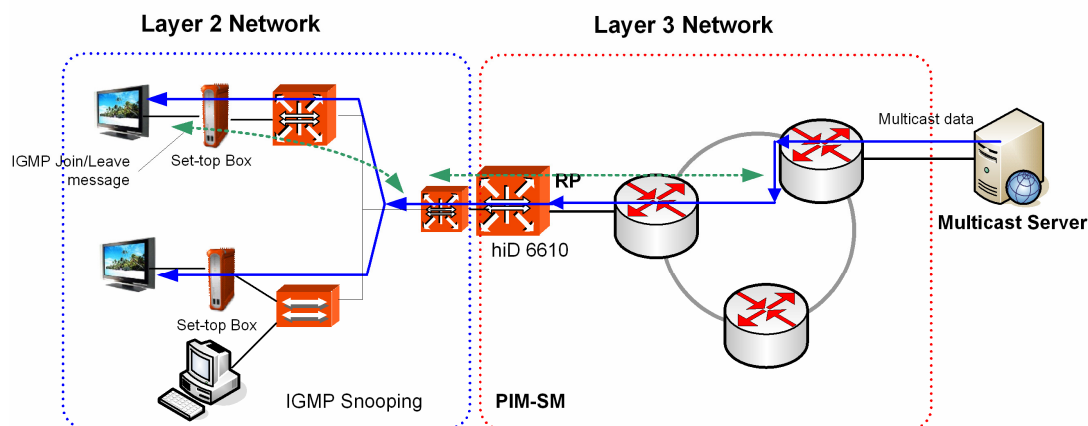


Fig. 9.2 PIM-SM Configuration Network

You can configure IGMP Snooping with PIM-SM as Fig. 9.3. If more than one port are on the same interface and the hiD 6610 S311 is located in Layer 3 boundary, IGMP Snooping and PIM-SM should be configured at the same time.

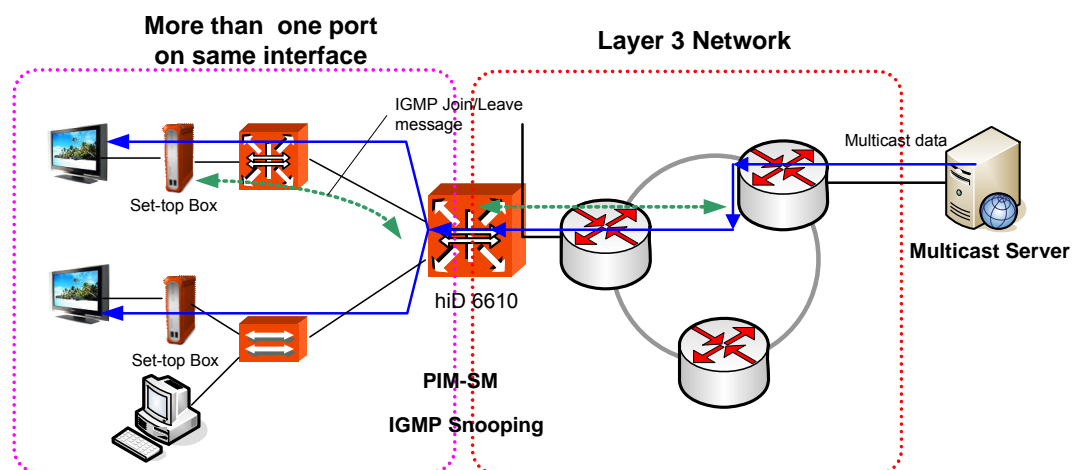


Fig. 9.3 IGMP Snooping and PIM-SM Configuration Network

9.1 Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) depends on hosts and routers that support multicasting. Whole system on a network is known which hosts belong to multicast groups. IGMP is not multicast routing protocol but group management protocol.

Multicast routers can receive the thousands of multicast packets from other group. If a router does not have any information of host membership, it has to broadcast the packets. This is bandwidth waste. To solve this problem, one group list of members is updated. IGMP helps multicast router to create and renew the list.

9.1.1 Enabling IGMP Snooping per VLAN

The hiD 6610 S311 supports 256 Snooping Membership Group Table that are managed by each VLAN. Snooping supports Enable/Disable by VLAN independently. By default, IGMP snooping is globally disabled on the switch.

To enable/disable global IGMP, use the following steps.

Step 1

Open *Global Configuration* mode using **configure terminal** command.

Step 2

Enable IGMP snooping in all existing VLAN interfaces.

Command	Mode	Description
ip igmp snooping	Global	Enables IGMP snooping globally
ip igmp snooping vlan <1-4094>		Enables IGMP snooping in VLAN interface

Step 3

To disable IGMP snooping, use the following command.

Command	Mode	Description
no ip igmp snooping	Global	Disables IGMP snooping globally
no ip igmp snooping vlan <1-4094>		Disables IGMP snooping in VLAN

To display global IGMP, use the following command.

Command	Mode	Description
show ip igmp snooping [vlan VLAN-ID]	Enable Global	Shows IGMP.snooping configuration.

9.1.2 IGMP v2 Snooping

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those associated with IP multicast devices. Internet Group Management Protocol (IGMP) is the internet protocol that helps to inform multicast groups to multicast router. In the multicast network, multicast router sends only IGMP query message that quest whether receive multicast packet when multicast packet is transmitted. If a switch sends the join message to multicast router, multicast router transmits the multicast packet only to that switch.

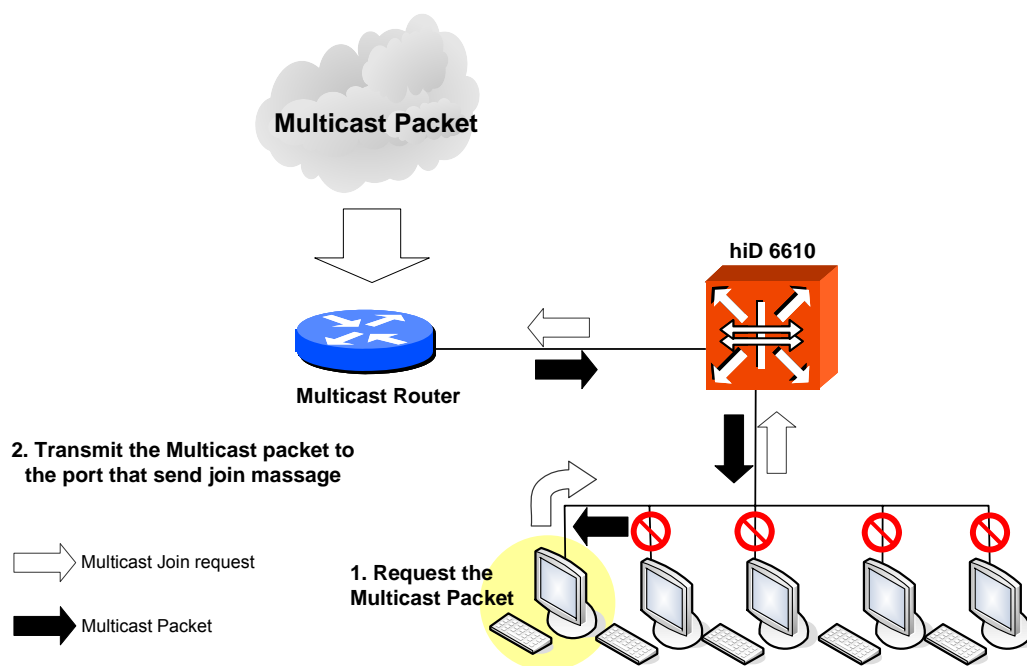


Fig. 9.4 IP Multicasting

IGMP Snooping is a function that finds port, which sends 「Join message」 to join in specific multicast group to receive multicast packet or 「Leave message」 to get out of the multicast group because it does not need packets.

Only when the switch is connected to multicast router, IGMP Snooping can be enabled.

9.1.2.1 IGMP v2 Snooping Fast Leave

If the Multicast client sends the leave message to leave out Multicast group, Multicast router sends IGMP Query message to the client again, and when the client does not respond, delete the client from the Multicast group.

In IGMP v2, even after Host sent Leave Message, it receives Multicast Traffic until sending Specific Query. In Snooping Fast-Leave Enable mode, it sends no more Multicast Traffic immediately by deleting from Membership Table at the time of receiving "Leave Message" without sending Specific Query.

Command	Mode	Description
ip igmp snooping fast-leave	Global	Takes away the host from Multicast group right after sending the leave message
ip igmp snooping fast-leave vlan <i>VLAN-ID</i>		Removes the host from Multicast group right after sending the leave message on a VLAN interface VLAN-ID: 1-4094

To disable IGMP snooping fast-leave, use the following command.

Command	Mode	Description
no ip igmp snooping fast-leave	Global	Disables IGMP snooping fast-leave function
no ip igmp snooping fast-leave vlan <i>VLAN-ID</i>		Disables IGMP snooping fast-leave function on a VLAN interface

To display IGMP snooping Immediate Leave configuration, use the following command.

Command	Mode	Description
show ip igmp snooping fast-leave [vlan <i>VLAN-NAME</i>]	Enable Global	Shows that the IGMP snooping Immediate leave is enabled.

9.1.2.2 IGMP v2 Snooping Querier

You can use the hiD 6610 S311 as IGMP querier without multicast router, because IGMP query daemon has been installed in the hiD 6610 S311. Legacy equipments used IGMP Querier of PIM but not developed Querier for IGMP Snooping. Because of this, to operate Querier on IGMP Snooping, IP Address was mandatory and Specific Query was operated by IGMP Querier.

The hiD 6610 S311 implemented IGMP Snooping Querier and it operates differently with IGMP Query. IGMP Snooping Querier can send General Query from Snooping Switch and it should be distinguished with Specific Query. IGMP Snooping Querier also uses Source IP Address 0.0.0.0, if there is no IP Address on Switch.

Enabling IGMP Snooping Querier

To enable the IGMP Snooping querier, use the following command.

Command	Mode	Description
ip igmp snooping querier	Global	Enables the IGMP snooping querier on the system.
ip igmp snooping querier vlan <i>VLAN-ID</i>		Enables the IGMP snooping querier on a VLAN interface. VLAN-ID: 1-4094

To disable IGMP querier, use the following command.

Command	Mode	Description
no ip igmp snooping querier	Global	Disables the IGMP snooping querier.
no ip igmp snooping querier vlan <i>VLAN-ID</i>		Disables the IGMP snooping querier on a VLAN interface. VLAN-ID: 1-4094

To display IGMP query parameter, use the following command.

Command	Mode	Description
show ip igmp snooping querier	Enable Global	Shows the IGMP snooping querier is enabled.
show ip igmp snooping querier vlan <i>VLAN-ID</i>		

9.1.2.3 IGMP v2 Snooping Last-Member-Interval

When receive Leave Message from host in IGMP v2, Queries sends Specific Query and check whether there is Multicast Group Member. Basically, if Membership Report about First Specify Query does not come, after 1 second, send second Specific Query. If there is no response also, it deleted from Membership Table. Last-member-interval is the value to regulate gap between first Specific Query and second Specific Query. By limiting Interval value, IGMP v2 function and fast Leave can be implemented.

To send IGMP Query message and configure the respond time, use the following command.

Command	Mode	Description
ip igmp snooping last-member-query-interval <100-10000>	Global	Configures the time of registering in multicast group after sending Join message on the system. (unit: ms)
ip igmp snooping last-member-query-interval <100-10000> vlan <i>VLAN-ID</i>		Configures the time of registering in multicast group after sending Join message on a VLAN interface.



If you configure **ip igmp snooping fast-leave**, it is meaningless to set the time as multicast group.

To release the waiting time for respond after sending IGMP Query message, use the following command.

Command	Mode	Description
no ip igmp snooping last-member-query-interval	Global	Returns to the default time of registering Join message in multicast group after sending it.
no ip igmp snooping last-member-query-interval vlan <i>VLAN-ID</i>		Returns to the default time of registering Join message after sending it on a VLAN interface.

To display IGMP query parameter, use the following command.

Command	Mode	Description
show ip igmp snooping last-member-query-interval	Enable Global	Shows the IGMP snooping query-interval configuration.
show ip igmp snooping last-member-query-interval vlan <i>VLAN-ID</i>		

9.1.2.4 Mrouter Port

Configuring the Mrouter Port per VLAN

You can designate, to which port, the multicast router is connected. If you designate multicast router is connected to where, it is possible to transmit multicast packet or message only to that port.

To designate the port connected to multicast router, use the following command.

Command	Mode	Description
ip igmp snooping mrouter port {<i>PORTS</i> <i>cpu</i>}	Global	Designates the port where multicast router is connected to on the system. <i>PORTS</i> : logical port number ID to use <i>cpu</i> : identifies the cpu port to use.
ip igmp snooping mrouter port {<i>PORTS</i> <i>cpu</i>} vlan <i>VLAN-ID</i>		Designates the port where multicast router is connected to on a VLAN interface.

To disable the port where multicast router is connected, use the following command.

Command	Mode	Description
no ip igmp snooping mrouter port {<i>PORTS</i> <i>cpu</i>}	Global	Disables the port where multicast router is connected on the system
no ip igmp snooping mrouter port {<i>PORTS</i> <i>cpu</i>} vlan <i>VLAN-ID</i>		Disables the port where multicast router is connected on a VLAN interface.

To display IGMP snooping mrouter configuration, use the following command.

Command	Mode	Description
show ip igmp snooping mrouter	Enable Global	Shows the mrouter configuration on the system.
show ip igmp snooping mrouter vlan <i>VLAN-ID</i>		Shows the mrouter configuration and detail information on a VLAN interface.

9.1.2.5 Displaying IGMP Snooping Statistics

To display an IGMP snooping statistics table, use the following command.

Command	Mode	Description
show ip igmp snooping state group <i>IP-ADDRESS</i>	Enable Global	Shows IGMP Snooping statistics information of Multicast group or ports or VLAN. PORTS: enters port number IP-ADDRESS: Multicast group IP address
show ip igmp snooping state port {<i>PORTS</i> <i>cpu</i>}		
show ip igmp snooping state vlan <i>VLAN-ID</i> <i>IP-ADDRESS</i>		

9.1.3 Multicast packets Filtering

When the switch receives multicast packets, the switch is supposed to transmit these packets according to IGMP table registration.

If you would like to block multicast packets when the packets are not registered on IGMP table, use the following command.

Command	Mode	Description
ip igmp multicast-filter	Global	Blocks whole packets if they are not registered on IGMP Table.
no ip igmp multicast-filter		Permits whole packets whether they are registered on IGMP Table or not.

9.1.4 IGMP Static Join Setting

If there is no group member on a network segment and you want to transmit multicast packet to that network segment, you can configure to pull multicast traffic down to a network segment using the **ip igmp static-group** command. With this command, the switch does not accept the packets, but forwards them. The outgoing interface appears in the IGMP cache, but the switch is not a member. Therefore, it can support fast switching.

To configure IGMP static Join, use the following command.

Command	Mode	Description
ip igmp static-group A.B.C.D1/M VLAN-ID PORT A.B.C.D2	Global	Configures IGMP static join setting. A.B.C.D1: IGMP group address VLAN-ID: <1-4094> PORT: enters port number A.B.C.D2: Reporter IP-address
no ip igmp static-group VLAN-ID		Disables the IGMP static join configuration. A.B.C.D1: IGMP group address VLAN-ID: <1-4094> PORT: enters port number A.B.C.D2: Reporter IP-address
no ip igmp static-group A.B.C.D1/M VLAN-ID no ip igmp static-group A.B.C.D1/M VLAN-ID PORT A.B.C.D2		

To see IGMP static Join group, use the following command.

Command	Mode	Description
show ip igmp static-group	Enable Global	Shows IGMP static join configuration

To register or delete Multicast group address on IGMP table static Join, use the following command on *Global Configuration* mode.

Command	Mode	Description
mac-address-table vlan VLANS static GROUP-ADDRESS port PORTS	Global	Registers multicast group address on IGMP table statically. VLANS: VLAN name GROUP-ADDRESS : Multicast group address PORTS: Selects port number
no mac-address-table vlan VLANS static GROUP-ADDRESS port PORTS		Deletes a specific multicast group address registered on IGMP table.

To remove all Multicast group addresses from IGMP table, use the following command.

Command	Mode	Description
clear mac-address-table-multicast vlan VLANS	Enable	Removes all multicast group addresses from the IGMP table



ip igmp static-group command offers a emulation of multicast group address that multicast address pretends to be joined, but it doesn't have any joined client. Otherwise, **mac-address-table** command help the switch send directly this information to the port as soon as the subscriber joins specified multicast group.

To see IGMP static Join group, use the following command.

Command	Mode	Description
show mac-address-table multi-cast vlan <i>VLANs</i>	Enable Global	Shows multicast group addresses on the IGMP table

9.1.5 Multicast VLAN Registration (MVR)

Multicast VLAN Registration (MVR) is for applications using wide-scale deployment of multicast traffic across an Ethernet ring-based service provider network. MVR allows a subscriber on a port to subscribe or not to a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network with subscribers remaining in separate VLANs. MVR helps to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

MVR assumes that subscribers subscribe or not (join and leave) these multicast streams by sending out IGMP join and leave messages. These messages can originate from an IGMP version-2-compatible host. Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independently of each other. One of them can be enabled or disabled without affecting the behavior of the other features. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping.

9.1.5.1 Enabling MVR

To enable/disable MVR, use the following steps.

Step 1

Enable IGMP snooping in the existing VLAN interfaces..

Step 2

Enable MVR function with the following command.

Command	Mode	Description
mvr	Global	Enables MVR on the system.
no mvr		Disables MVR on the system.

9.1.5.2 MVR Group Address

Statically configure a VLAN interface to receive multicast traffic sent to the multicast VLAN and the IP multicast address. An interface statically configured as a member of a group remains a member of the group until statically removed.

Command	Mode	Description
mvr vlan <i>VLAN-ID</i> group <i>GROUP-ADDR</i>	Global	Configures MVR group address. GROUP-ADDR: specific group address (ex: a.b.c.d or a.b.c.d-x.y.z.w)

To delete the statically configured MVR group address, use the following command.

Command	Mode	Description
no mvr vlan <i>VLAN-ID</i> group <i>GROUP-ADDR</i>	Global	Deletes a MVR group address. GROUP-ADDR: specific group address (ex: a.b.c.d or a.b.c.d-x.y.z.w)

9.1.5.3 MVR IP Address

Statically configure a VLAN interface to receive multicast traffic sent to the multicast VLAN and the IP multicast address. An interface statically configured as a member of a group remains a member of the group until statically removed.

When a multicast server belongs to different network from user's network, a multicast router operates as Layer 3 forwarding for each MVR VLAN. In this case, when an IGMP packet of a subscriber is transmitted to the multicast server, a source address of the IGMP packet may not match the network address of MVR VLAN. To handle such a problem, you can replace a source address of an IGMP packet with one of the IP addresses of MVR VLAN.

To configure a helper address to replace a source address of an IGMP packet, use the following command.

Command	Mode	Description
mvr vlan <i>VLAN-ID</i> helper <i>IP-ADDRESS</i>	Global	Configures MVR Ip address. IP ADDRESS: specific IP address of MVR VLAN helper

To delete the configured MVR VLAN helper IP address, use the following command.

Command	Mode	Description
no mvr vlan <i>VLAN-ID</i> helper	Global	Deletes a MVR Ip address.

9.1.5.4 Send and Receive Port

Statically configure a VLAN interface to receive multicast traffic sent to the multicast VLAN and the IP multicast address. An interface statically configured as a member of a group remains a member of the group until statically removed.

Command	Mode	Description
mvr port <i>PORTS</i> type { receiver source }	Global	Identifies the logical port's type either MVR receiver port or source port. PORTS: logical port number

- Source**
This configures uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. All source ports on a switch belong to the single multicast VLAN.
- Receiver**
This configures a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the

multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN.

To delete the statically configured MVR port, use the following command.

Command	Mode	Description
no mvr port <i>PORTS</i>	Global	Deletes a MVR port.

9.1.5.5 Displaying MVR Configuration

To display an MVR configuration, use the following command.

Command	Mode	Description
show mvr	Enable Global	Shows a MVR configuration.
show mvr port		
show mvr vlan <i>VLAN-ID</i>		

9.1.6 IGMP Filtering and Profile

With the IGMP filtering feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only group specific query and membership reports, including join and leave reports. It does not control general IGMP queries. IGMP filtering has no relationship with the function that directs the forwarding of IP multicast traffic.

9.1.6.1 Creating IGMP Profile

You can create or modify the IGMP profile to be used for filtering IGMP join requests from a port. The system prompt will be changed to SWITCH(config-igmp-profile[1])# from SWITCH(config)#.

To create/delete IGMP profile, use the following command.

Command	Mode	Description
ip igmp profile <1-4294967295>	Global	Creates IGMP profile. 1-4294967295: profile number
no ip igmp profile <1-4294967295>		Deletes IGMP profile

To display the IGMP profile, use the following command.

Command	Mode	Description
show ip igmp profile [<1-4294967295>]	Enable Global	Shows IGMP profile.

9.1.6.2 Group Range of IGMP Profile

Configure the group range of IGMP Profile using the following command.

Command	Mode	Description
range <i>A.B.C.D1</i> [<i>A.B.C.D2</i>]	IGMP Profile	Configures a group range of IGMP profile A.B.C.D1: Start IP multicast address A.B.C.D2: End IP multicast address
no range <i>A.B.C.D1</i> [<i>A.B.C.D2</i>]		Deletes a configured group range

9.1.6.3 IGMP Profile Policy

Configure the action to permit/deny access to the IP multicast addresses using the following command.

Command	Mode	Description
{permit deny}	IGMP Profile	Configures the action of IGMP profile policy whether it denies/permits the matching addresses.

9.1.6.4 Applying IGMP Profile to the Filter Port

To apply the configured IGMP Profile to the filter port, use the following command.

Command	Mode	Description
ip igmp filter port <i>PORTS</i> profile <1-4294967295>	Global	Configures IGMP profile. PORTS: port number 1-4294967295: number of configured IGMP profile

To cancel the applying of the profile, use the following command.

Command	Mode	Description
no ip igmp filter port <i>PORTS</i>	Global	Disables an applied IGMP profile. PORTS: port number

To display the IGMP filter configuration, use the following command.

Command	Mode	Description
show ip igmp filter port <i>PORTS</i>	Enable Global	Shows a configuration.

9.1.6.5 Max Number of IGMP Join Group

You can configure the maximum number of IGMP groups that a Layer 2 interface can join. To configure the maximum number of IGMP groups per port, use the following command.

Command	Mode	Description
ip igmp max-groups port <i>PORTS</i> count <0-4294967295>	Global	Configures the maximum number of IGMP groups. PORTS: port number 0-4294967295: maximum number of IGMP groups that the port can join

To return to the default setting, use the following command.

Command	Mode	Description
no ip igmp max-groups port <i>PORTS</i>	Global	Returns to the default of no maximum. PORTS: the number of port

9.2 PIM-SM (Protocol Independent Multicast-Sparse Mode)

IGMP is the protocol to help multicast communication between switch and host, but PIM is the protocol for multicast communication between router and router. There are two kinds of PIM, PIM-DM (Protocol Independent Multicast–Dense Mode) and PIM-SM (Protocol Independent Multicast–Sparse Mode), the hiD 6610 S311 supports PIM-SM only.

Protocol of dense mode can send information about data packet and member to interface, which is not connected to multicast source or receiver, and multicast router saves connection state to all the nodes. In this case, when most hosts are belonged to multicast group and there is enough bandwidth to support flow of controlling message between constituent members, these overheads are acceptable, but the other cases are inefficient.

Contrary to dense mode, PIM-SM receives multicast packet only when request comes from specific host in multicast group. Therefore PIM-SM is proper when constituent members of group are dispersed in wide area or bandwidth used for the whole is small. Sparse mode is the most useful on WAN and can be used on LAN. For standard of PIM-SM, you can refer to RFC 2362.

RPT and SPT

RP (Rendezvous Point) works in a central role for PIM-SM. Viewing the below chart, multicast packet is transmitted to D as RP from A as source, through B and C. And D (RP) transmits multicast packet after receiving join message from E or F. That is, all multicast packets are transmitted with passing through RP (Rendezvous Point). For instance, even though F needs multicast packet, the packet is passed through 『A→B→C→D→C→F』, not 『A→B→C→F』.

Like this, route made with focusing on RP is RPT (Rendezvous Point Tree) or shared tree. There is only one RP in one multicast group. RPT has (*, G) entry because receiver can send a message to RP without knowing source. “G” means multicast group.

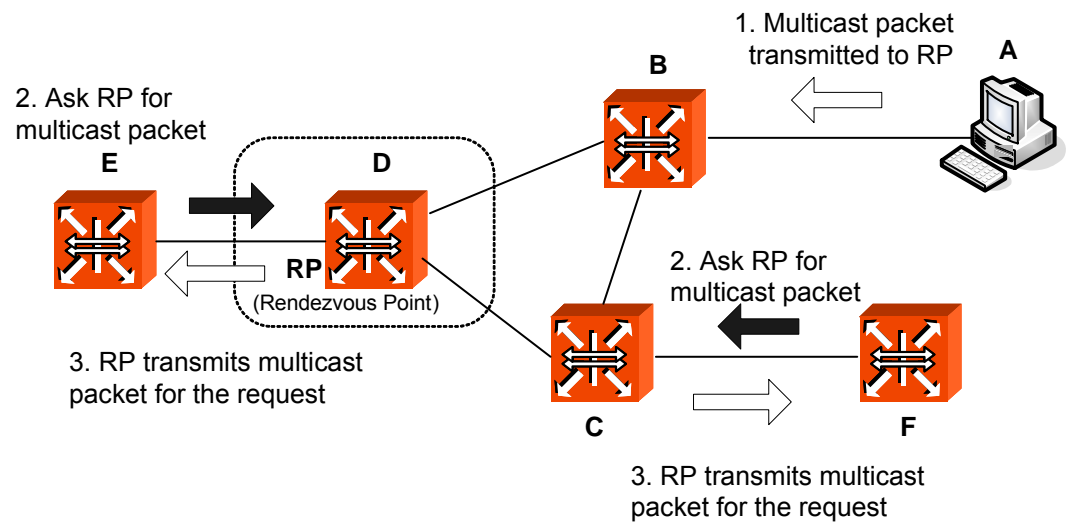


Fig. 9.5 RPT of PIM-SM

Also, routers on packet route automatically optimize route by deleting unnecessary hops when traffic exceeds certain limit. After route to source and multicast group connected to the source are constituted, all sources have route to connect to receiver directly.

In the below figure, packets are usually transmitted through 『A→B→C→D』, but packets are transmitted through faster route 『A→C→F』 when traffic is increased. SPT (Shortest-Path Tree) selects the shortest route between source and receiver regardless of RP, it is called source based tree or short path tree. SPT has (S, G) entry, “S” means source address and “G” means multicast group.

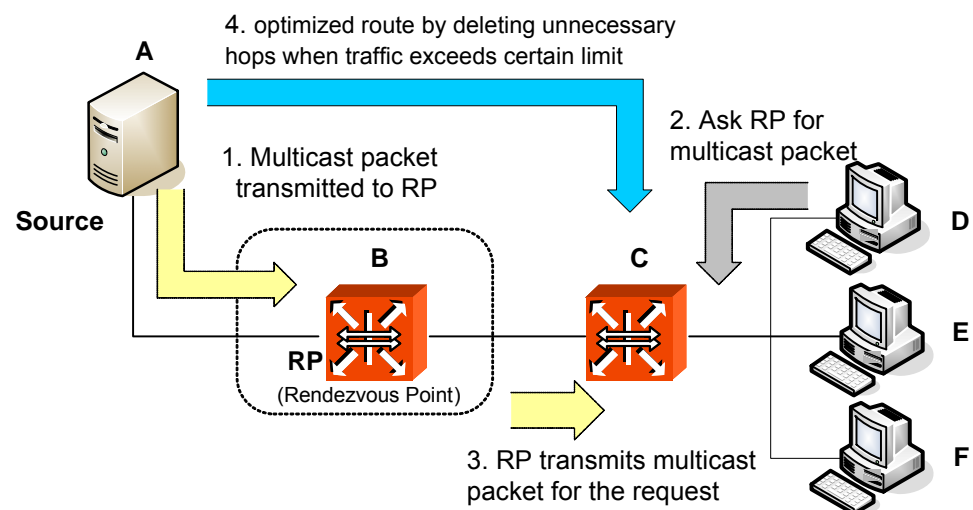


Fig. 9.6 STP of PIM-SM

9.2.1 Enables PIM Configuration

To activate the PIM-SM, use the following command.

Command	Mode	Description
router pim	Global	Enables PIM-SM and enters PIM configuration mode.
no router pim		Disables PIM-SM.



PIM-SM supports both IGMP queries and IGMP Snooping, therefore you're not able configure them at the same time.

9.2.2 BSR and RP

There are two ways to decide RP as central of PIM-SM on multicast network. One is that network administrator manually decides RP and the other way is that RP is automatically decided by exchanging information between multicast routers installed on network. The information transmitted between multicast routers in the automatic way is called Bootstrap message and the router, which sends this Bootstrap message, is called BSR (Bootstrap Router). All PIM routers existing on multicast network can be BSR.

Routers that want to be BSP are named as candidate-BSR and one router, which has the highest priority, becomes BSR among them. If there are routers, which have same priority, then one router, which has the highest IP address, becomes BSR. Bootstrap message includes priority to decide BSR, hash-mark to be used in Hash, and RP information. After deciding BSR, routers, which support RP, transmit candidate-RP message to BSR. Candidate-RP message includes priority, IP address, and multicast group. Then BSR adds candidate-RP message to Bootstrap message and transmits it to another PIM router. Through this transmitted Bootstrap message, RP of multicast group is decided. User's equipment belonged in PIM-SM network can be candidate-BSR and BSR is decided among them. Candidate-BSR transmits Bootstrap message to decide BSR. You can configure priority to decide BSR among Bootstrap messages and Hash-mask.

9.2.2.1 Configuring Static RP

To configure static RP manually, use the following command.

Command	Mode	Description
static-rp <i>A.B.C.D/M A.B.C.D</i>	PIM	Configures RP of multicast group A.B.C.D/M : Group prefix A.B.C.D: IP address of RP
no static-rp <i>A.B.C.D/M A.B.C.D</i>		Deletes RP configured by network administrator.

To delete rp-mapping, use the following command.

Command	Mode	Description
clear rp-mapping { <i>A.B.C.D</i> all}	PIM	Deletes RP mapping of specific IP address or all of them A.B.C.D: IP address of RP

9.2.3 Bootstrap Router (BSR) Information

The information transmitted between multicast routers in the automatic way is called Bootstrap message and the router, which sends this Bootstrap message, is called BSR (Bootstrap Router). All PIM routers existing on multicast network can be BSR. Routers, which want to be BSP, are named candidate-BSR and one router, which has the highest priority, becomes BSR among them. If there are routers, which have same priority, then one router, which has the highest IP address, becomes BSR.

It is possible to configure the following messages, which are included in candidate-BSR message.

Since it is possible to assign several IP addresses in hiD 6610 S311, the switch may have several IP addresses assigned. User can select one IP address among several IP addresses to be used in switch as candidate-BSR.

9.2.3.1 IP Address of candidate-BSR

To configure candidate-BSR, use the following command.

Command	Mode	Description
cand-bsr address <i>IP-ADDRESS</i>	PIM	Assigns IP address for using at Candidate-BSR.

To disable assigned IP address in candidate-BSR, use the following command.

Command	Mode	Description
no cand-bsr address	PIM	Disables .the configuration for bsr-candidate.

9.2.3.2 Priority of candidate-BSR

If you decide BSR among candidate-BSRs, priority in Bootstrap message is compared to decide it. The highest priority of candidate-BSR becomes BSR.

To configure priority of Bootstrap message, use the following command.

Command	Mode	Description
cand-bsr priority <0-255>	PIM	Configures the priority of Bootstrap message.
no cand-bsr priority		Delete the priority configuration of Bootstrap message.

9.2.3.3 Hash-mask of candidate-BSR

When there are same priorities to compare candidate-BSR, IP address is compared through Hash. User can configure Hash-mask to apply Hash.

When hiD 6610 S311 becomes the candidate-BSR, user can configure Hash-mask included in Bootstrap message. Use the following command.

Command	Mode	Description
cand-bsr hash-mask <0-32>	PIM	Configures Hash-mask on Bootstrap message.
no cand-bsr hash-mask		Removes Hash-mask on Bootstrap message.

9.2.4 RP Information

After deciding BSR on multicast network, candidate-RP routers send RP message to BSR. Candidate-RP message includes priority, IP address, and multicast group. Then, BSR adds the received candidate-RP information to Bootstrap message and transmit to another PIM router. Through this Bootstrap message, RP of multicast group is decided. All routers belonged in multicast network can become candidate-RP and routers which generally consist candidate-BSR are supposed to consist candidate-RP. It is possible to configure the following information, which is included in candidate-RP message.

9.2.4.1 IP address of Candidate RP

You can configure several IP addresses on the hiD 6610 S311. Therefore, you need to decide which IP address to be used as candidate-RP. This command is used to statically configure the RP address for multicast groups.

To configure IP address to be used in candidate-RP, use the following command.

Command	Mode	Description
cand-rp address <i>A.B.C.D</i>	PIM	Configures RP address for multicast groups statically. A.B.C.D: Multicast group Address

- If RP-address configured through BSR and RP-address configured statically are both available for a group range, the RP-address configured through BSR is chosen.
- If multiple static-RPs are available for a group range, then one with the highest IP address is chosen.

To delete configured IP address, use the following command.

Command	Mode	Description
no cand-rp address	PIM	Deletes configured IP address.

9.2.4.2 Multicast Group Registration

Use this command to give the router the candidate RP status using the IP address of the specified interface.

Command	Mode	Description
cand-rp group <i>A.B.C.D/A</i>	PIM	Registers multicast group IP address belong to RP candidate. A.B.C.D: Multicast group Address includes RP candidate.
no cand-rp group <i>A.B.C.D/A</i>		Deletes the multicast group IP address belong to RP candidate.

9.2.4.3 Priority of Candidate-RP

Use this command to give the router the candidate RP status using the IP address of the specified interface.

Command	Mode	Description
cand-rp priority <0-255>	PIM	Configures priority value for a RP candidate. 0-255: Priority value
no cand-rp priority		Deletes configured priority value of RP candidate.

9.2.4.4 Interval of Candidate-RP

Use this command to give the router the candidate RP status using the IP address of the specified interface.

Command	Mode	Description
cand-rp interval <1-65535>	PIM	Configures C-RP advertisement interval for a RP candidate. 1-165535: Interval in seconds (Default value: 60 seconds)
no cand-rp interval		Deletes interval to transmit candidate-RP message

9.2.4.5 Candidate-RP Message of other members

One network may include different multicast groups and routers that are not members of multicast group. Therefore, it can happen that routers, which are members of another network or not members of multicast group, apply for RP and transmit candidate-RP message.

In order to prevent this case, user can block candidate-RP message of another router by making only candidate-RP in multicast group communicate. In order to block candidate-RP message from routers which are not members, perform the below tasks.

Step 1

Use the following command to deny all packets which trying to transmit on network.

Command	Mode	Description
cand-rp access deny A.B.C.D/A	PIM	Blocks all packets transmission on specified network
no cand-rp access deny A.B.C.D/A		Removes the blocking configuration

Step 2

Allow only the transmitted packets by routers that exchange candidate-RP message.

Command	Mode	Description
cand-rp access permit A.B.C.D/A	PIM	Allows only packets transmission by routers that will exchange candidate-RP.
no cand-rp access permit A.B.C.D/A		Releases allowed packet configuration.

9.2.5 Assert Message Information

When there are several PIM-SM routers on same LAN, they may exchange packets are not needed. In order to prevent this problem, you need to assign one PIM-SM router to transmit multicast packet. In this case, assigned router is named Assert.

For example, there are router B, C which can transmit multicast packets in case of receiving Join message from receiver. D and E, which send Join message, cannot decide which router to receive.

And C may transmit same packet to B belonged in multicast group. In this case, if Assert is decided, multicast group is well organized because D and E transmit Join message only to Assert. When Assert is decided, Metric and Preference in Assert message are compared. Lower Metric has priority and higher Preference has priority.

9.2.5.1 Metric

To configure Metric of Assert message, use the following command.

Command	Mode	Description
metric <1-2147483647>	PIM	Configures Metric of Assert message.
no metric		Deletes configured Metric of Assert message.

9.2.5.2 Preference

To configure Preference of Assert message, use the following command.

Command	Mode	Description
preference <1-2147483647>	PIM	Configures preference of Assert message.
no preference		Deletes configured preference of Assert message.

9.2.5.3 Configuring Assert Message on specified interface

If there is a network environment that needs Assert, Assert message is compared to decide Assert. It is possible to configure Assert message information owned only by Ethernet interface in which PIM-SM is configured.

To configure Assert message information on Ethernet interface, use the following command.

Command	Mode	Description
ip pim metric <1-127>	Interface	Configures metric of Assert message of specific interface
ip pim preference <1-255>		Configures preference of Assert message of specific interface
ip pim threshold <1-255>		Configures threshold of Assert message of specific interface

To delete configured Assert message information on Ethernet interface, use the following commands.

Command	Mode	Description
no ip pim metric	Interface	Deletes configured metric of Assert message of specific interface.
no ip pim preference		Deletes configured preference of Assert message of specific interface.
no ip pim threshold		Deletes configured threshold of Assert message of specific interface

9.2.6 Cisco Router Interoperability

9.2.6.1 Checksum of Full PIM Register Message

Although source of multicast is not connected to multicast group, multicast communication is possible. In the below picture, First-Hop router directly connected to source can receive packet from source without (S, G) entry about source.

The First-Hop router encapsulates the packet in Register message and unicast to RP of multicast group. RP encapsulates capsule of Register message and transmits it to members of multicast group.

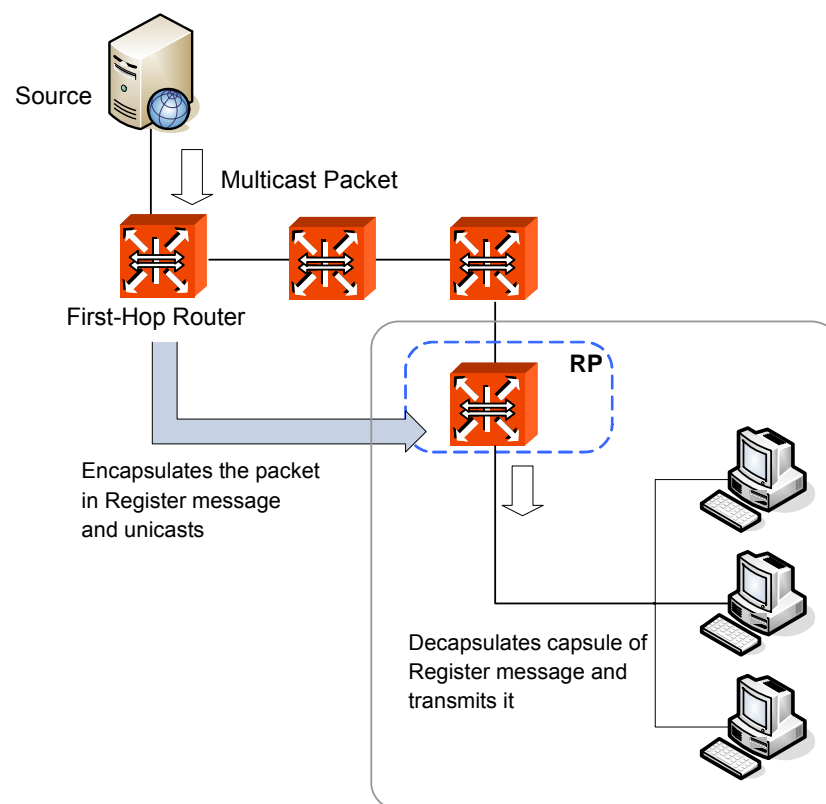


Fig. 9.7 In Case Multicast Source not Directly Connected to Multicast Group

When the Register message is transmitted, the range of Checksum in header conforms to header part as RFC standard, but whole packet is included in the range of checksum in case of Cisco router. For compatibility with Cisco router, you should configure the range of Checksum of Register message as whole packet.

To configure the range of Checksum of Register message as whole packet for compatibility with Cisco router, use the following command.

Command	Mode	Description
whole-packet-checksum	PIM	Configures Join/Prune timer value. 1-65535: interval (unit: second)
no whole-packet-checksum		Disables TX interval configuration.



This command is disabled by default. And Register Checksum is calculated only over the header by default.

9.2.7 Interval of Cache-check

RP receives packet from multicast source and transmits it to receiver. However, if there is no packet received from source for certain period, it is not necessary to keep multicast item. Therefore, RP checks whether packet is received from source at regular interval and this function is named Cache-check. In order to configure the interval of Cache-check, use the following command.

Command	Mode	Description
cache-check interval <1-128>	PIM	Configures the interval of Cache-check. (Default value: 20 seconds)
no cache-check interval		Deletes configured interval of Cache-check.

9.2.8 Multicast Routing Table

There is RPF (Reverse Path Forwarding) on route of transmitting multicast packet. RPF is, a former router that transmits multicast packet. User can configure specified router as RPF by configuring routing table manually.

To set multicast routing table manually to configure RPF, use the following command.

Command	Mode	Description
mroute A.B.C.D/M A.B.C.D	PIM	Configures RPF about packets of specified multicast group.

To delete configured multicast routing table, use the following command.

Command	Mode	Description
no mroute A.B.C.D/M [A.B.C.D]	PIM	Deletes the configured multicast routing table.
no mroute all		Deletes all multicast routing tables.

9.2.9 PIM-SM on Ethernet Interface

You need to open *Interface Configuration* mode of specified interface first for activating PIM-SM on Ethernet interface. To open *Interface Configuration* mode, use the following command.

Command	Mode	Description
interface <i>INTERFACE</i>	Global	Opens <i>Interface Configuration</i> mode of specified interface.

To disable *Interface Configuration* mode, use the following command.

Command	Mode	Description
no interface <i>INTERFACE</i>	Global	Disables a specified interface.

9.2.9.1 PIM-SM and Sparse Mode

To activate PIM-SM after opening the *Interface Configuration* mode, use the following command.

Command	Mode	Description
ip pim sparse-mode	Interface	Activates PIM-SM on specified interface.

To disable PIM-SM, use the following command.

Command	Mode	Description
no ip pim sparse-mode	Interface	Disables PIM-SM from specified interface.

9.2.9.2 Blocking Multicast packets

It may happen that some of receivers in multicast group cannot receive packet because of not satisfying terms to receive multicast packet. It is possible to configure not to receive multicast packets that can not be sent to receiver.

To block transmitting packet to specified multicast group, use the following command.

Command	Mode	Description
ip pim access-list <i>A.B.C.D/A</i>	Interface	Blocks the packets which trying to transmit from specified multicast group. A.B.C.D/A : Multicast group address prefix
no ip pim access-list <i>A.B.C.D/A</i>		Release blocked multicast group. A.B.C.D/A : Multicast group address prefix

9.2.9.3 Blocking Bootstrap message

When all switches' configured PIM are considered as one big PIM domain, it may cause that unnecessary Bootstrap messages can be transmitted between group members which are operated as different service, and then it results to confuse to decide RP.

To prevent this problem, you can prohibit transmitting Bootstrap message between multi-cast groups, which are operated as different service.

To prohibit transmitting Bootstrap message between multicast groups, which are operated as different service, use the following command.

Command	Mode	Description
ip pim border	Interface	Blocks the Bootstrap message which trying to be transmitted.
no ip pim border		Release blocked Bootstrap message.

9.2.10 Displaying PIM-SM Information

9.2.10.1 Multicast Routing Table

To display the information of multicast routing table, use the following command.

Command	Mode	Description
show ip pim mrt detail	Enable Global	Shows multicast routing table in detail
show ip pim mrt group A.B.C.D		Shows multicast routing table of specified multicast group A.B.C.D: group address
show ip pim mrt summary		Shows the summary of multicast routing table
show ip pim mroute		Shows PIM multicast router information.

9.2.10.2 RP Table

To see RP table registered by the switch, use the following command.

Command	Mode	Description
show ip pim rp	Enable Global	Shows PIM RP table which has been registered A.B.C.D: multicast group address
show ip pim rp group A.B.C.D		Shows the registered RP table in specified multicast group A.B.C.D: group address

9.2.10.3 PIM-SM of Ethernet Interface

To see the information of PIM on Ethernet interface, use the following command.

Command	Mode	Description
show pim interface	Enable Global	Shows PIM interface information.

9.2.10.4 Statistics and neighbor router

To display IP PIM packet statistics, use the following command.

Command	Mode	Description
show ip pim statistics	Enable	Shows IP PIM statistics of multicast packets.
show ip pim neighbor	Global	Shows PIM neighbor routers.

9.2.10.5 PIM Debug

To activate PIM-SM debugging, use the following command.

Command	Mode	Description
debug pim all	Enable	Activates PIM debugging. all : all PIM debugging
debug pim igmp		Enables the PIM igmp debugging.
debug pim neighbors		Enables the PIM neighbor's information debugging.
debug pim mrt		Enables multicast routing table debugging.
debug pim proto		Shows the information of PIM packets' transmission.
debug pim proto-detail		Shows the PIM packets' route how to be transmitted.
debug pim timer		Enables the PIM timer's debugging.
debug pim register		Enables the PIM-SM register timer's debugging.

To release PIM debugging configuration, use the following command.

Command	Mode	Description
no debug pim {all igmp mrt neighbors proto proto-detail timer register}	Enable	Disables PIM debugging.

To show debugging information of PIM, use the following command.

Command	Mode	Description
show debugging pim	Enable	Show the configured information for PIM debugging.

10 IP Routing Protocol

10.1 Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is, as defined in RFC 1163, 1267, Exterior Gateway Protocol (EGP) to connect to exterior Network. BGP manages routing information in network so that Autonomous System (AS) can transmit and receive routing information. BGP consists of network number, which packet is passed through and autonomous system number. The hiD 6610 S311 supports BGP version 4 defined in RFC 1771. BGP version 4 provides Aggregate route by using Classless Inter-domain Routing (CIDR) to reduce size of routing table. CIDR provides IP prefix, which is network address instead of IP address on BGP network. OSPF and RIP can also transmit CIDR path.

Switch, which takes BGP protocol, is intended to exchange AS and path reaching to AS between BGP equipments. By doing it, user can prevent routing Loop and take the most effective AS information.

You can configure Multi Exit Discriminator (MED) by using route map. When new routing information is transmitted to neighbor BGP, MED is passed without any change. Thus, BGP routers located in same AS can select path with same standard.

10.1.1 Basic Configuration

BGP configuration is roughly divided into basic configuration and advanced configuration. Basic configuration includes the following.

- BGP Routing
- AS Route Filtering
- BGP Filtering through Prefix Lists

10.1.1.1 BGP Routing

To activate the BGP router, use the following command.

Command	Mode	Description
router bgp <1-65535>	Global	Assigns AS number to configure BGP routing, enter the AS number.

AS number is an identification of autonomous system used for detecting the BGP connection. AS number 65512 through 65535 are defined as private AS number. Private number cannot be advertised on the config Internet.

10.1.1.2 AS Route Filtering

As filtering information with network address on BGP network, it is possible to filter information going through AS. Policies applied to decide route are registered in access list. To filter routing information with AS standard, configure filtering policy in access list and apply the policy to neighbor router.

Define specific AS in access list.

Command	Mode	Description
ip as-path access-list <i>WORD</i> { permit deny } <i>LINE</i>	Global	Defines specific AS in access list: WORD: enter the access list number. LINE: enter the expression.

10.1.1.3 BGP Filtering through Prefix Lists

When you restrict BGP route, prefix list is preferred than access list because of the following reasons:

- Saving time to search and apply data in case of massive filter lists
- Unlimited registration in filter lists
- Easy to use

Before applying prefix list, user should configure prefix list. User can assign number to each policy registered in prefix list.

Traffic Filtering Operation through Prefix Lists

Filtering through prefix list processes routing information in specific order by applying policy defined in filter list. It is similar to access list but there are more detail rules as follow.

- Allows all network information if there is no defined policy in prefix list.
- Rejects specified network information unless policy applied to network is defined in prefix list.
- Distinguishes each policy with the assigned number and applies policy which has the lowest number when there are more than one policy applied to one network.

Routers search policy in prefix list from the top in order. When they find required policy, they stop searching. For faster operation, user can make quick search list on the top of the list by using **seq** provided from **ip prefix-list**. In order to view assigned number to policy, use the command, **show ip prefix-list**.

Policies configured by user are automatically assigned number. If you do not configure it, you should assign number to each policy by using the command, **ip prefix-list seq**.

Creating Prefix List

To create prefix list, use the following command.

Command	Mode	Description
ip prefix-list <i>NAME</i> {deny permit} {any A.B.C.D/M [ge <0-32>] [le <0-32>]}	Global	Creates a prefix list to be applied.
ip prefix-list <i>NAME</i> description <i>DESCRIPTION</i>		Adds a description to a created prefix list.



To create prefix list, you should select **permit** or **deny**.

Creating Prefix List Policy

You can add policy to prefix list one by one. Use the following command.

Command	Mode	Description
ip prefix-list <i>NAME</i> seq <1-4294967295> {deny permit} {any A.B.C.D/M [ge <0-32>] [le <0-32>]}	Global	Configures policy of prefix list and assigns number to the policy.

You can input **ge** and **le** optionally, and they are used when you configure more than one network. If you do use neither **ge** nor **le**, network range is more clearly configured. When only **ge** attribute is configured, network range is configured from **ge** value, and when only **le** attribute is configured, network range is configured from netmask to **le** value.

Displaying Prefix List Policy

To display information about prefix table, use the following command.

Command	Mode	Description
show ip prefix-list [detail summary] [<i>NAME</i>]	Enable Global	Shows the prefix list. detail: detail list summary: brief list NAME: enter the prefix name.
show ip prefix-list <i>NAME</i> A.B.C.D/M [longer first-match]		Shows a policy of the prefix list applied to the specified network. longer: all policies first-match: first applied policy
show ip prefix-list <i>NAME</i> seq <1-4294967295>		Shows a policy of the specified number.

Deleting Number of Inquiring Prefix List

By default system records number how many times prefix list is inquired. To delete the number, use the following command.

Command	Mode	Description
clear ip prefix-list <i>NAME</i> [<i>A.B.C.D/M</i>]	Enable Global	Deletes the number how many times prefix list is inquired.

10.1.2 Advanced Configuration

After finishing basic configuration, it is possible to do advanced configuration. It contains the following sections.

- BGP Community Filtering
- Displaying and Managing BGP

10.1.2.1 BGP Community Filtering

BGP supports transmit policy distributing routing information. Distributing routing information is operated based on not only community list but also IP address and AS route. Community list makes community according to each destination and routing policy is applied based on community standard.

It helps configure BGP speaker that distributes routing information.

Community is destination group that shares some common attributes. One destination can be belonged to more than one community. As administrator can configure to which community destination is belonged. By default, all destinations are configured to be in internet community.

The other defined and well-known communities are as the below.

- **no-export:**
Do not distribute this route to exterior BGP neighbor router.
- **no-advertise:** (either exterior or interior)
Do not distribute this route to neighbor router.
- **local-as:**
Distribute this information to neighbor routers of low level AS located on BGP united network. Do not distribute it to exterior router.

To create community list, use the following command.

Command	Mode	Description
ip community-list <i>NAME</i> { permit deny } { community local-AS no-advertise no-expert }	Global	Creates a community list.

community is notated with a form, AA:NN as defined in RFC. AA is AS number and NN is number of 2 bytes.

10.1.2.2 Displaying and Managing BGP

You can delete all factors of cache, table and database. In addition, it is possible to display specific statistics.

Deleting Cache, Table and Database

You can delete all contents of specific cache, table, and database when some factors are invalid or unreliable.

To delete cache, table or database, use the following command.

Command	Mode	Description
clear ip bgp {* ip-address asnumber} [in out soft [in out]]	Enable Global	Reconfigures information about BGP neighbor router, AS group, all (*) BGP connections.

Displaying System and Network Statistics

You can display specific statistics such as contents of BGP routing table, cache, and database. Information provided can be used to determine resource utilization and solve network problems.

You can also display information about node reach ability and discover the routing path your device's packets are taking through the network.

To display various routing statistics, use the following command.

Command	Mode	Description
show ip bgp prefix-list <i>NAME</i>	Enable Global	Shows peers to which the prefix has been advertised.
show ip bgp cidr-only		Shows all BGP routes including subnetwork and upper network.
show ip bgp community [number local-AS no-advertise no-export]		Shows route belonged in specific community. Community Number is formed as AA:NN.
show ip bgp community-list <i>WORD</i> [exact-match]		Shows all routes that are permitted by the community list, enter the WORD value.
show ip bgp community-info		Shows all information of BGP community.
show ip bgp filter-list <i>WORD</i>		Shows routes that are matched by the specified autonomous system route in access list, enter the WORD value
show ip bgp regexp <i>LINE</i>		Shows routes that match the specified regular expression entered on the command line, enter the LINE value.
show ip bgp attribute-info		Shows all information of BGP attributes.
show ip bgp neighbors [ip-address]		Shows detail information on TCP and BGP connections to individual neighbors.

Command	Mode	Description
show ip bgp neighbors ip-address [advertised-routes received-routes routes]	Enable Global	Shows information about the TCP and BGP connections to neighbors. The advertised-routes option displays all the routes the router has advertised to the neighbor. The received-routes option displays all received routes (both accepted and rejected) from the specified neighbor. The routes option displays all routes that are received and accepted.
show ip bgp paths		Shows all BGP routes in database.
show ip bgp summary		Shows all BGP connections.

10.2 Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is an interior gateway protocol developed by the OSPF working group of Internet Engineering Task Force (IETF). OSPF designed for IP network supports IP subnetting and marks on information from exterior network.

Moreover, it supports packet authorization and transmits/receives routing information through IP multicast. It is most convenient to operate OSPF on layered network.

The first thing you should do on OSPF network is to configure border router and AS boundary router. And then, you need to configure basic setting to operate OSPF router and interface in area.

When you customize OSPF router for user's environment, you have to check that all configurations are same in each router.

10.2.1 Enabling OSPF

To configure routing protocol, use the following command.

Command	Mode	Description
router ospf <1-65535>	Global	Opens <i>Router Configuration</i> mode.

10.2.2 OSPF Network Type

OSPF provides three types of the network as the follow:

- Broadcast Network
- Non-broadcast Multi-access (NBMA) Network
- Point-to-point Network.

It is possible to configure OSPF network as broadcast type or non-broadcast type. For example, if user's network does not support multicasting, it is possible to configure broadcast network as non-broadcast type. Conversely, it is also possible to configure NBMA network such as frame relay as broadcast type.

To operate network as NBMA type, all routers should be connected through virtual circuit. However, it is possible to connect to some part of OSPF network with using virtual circuit through point-to-multipoint function so that network management cost can be saved. Two routers that are not directly connected should transmit and receive routing information

through intermediate router. So, you do not have to configure neighbor router anymore.

The followings are features of OSPF point-to-multipoint type.

- IP source is economized because you do not have to assign Neighbor router and there is no additional process to configure designated router.
- Management cost is saved because it does not need to be linked with all router on network like a spider's thread.
- It can provide more stable network service since it can communicate even when virtual circuit is disconnected.

To configure OSPF network type, use the following command.

Command	Mode	Description
ip ospf network {broadcast non-broadcast {point-to-multipoint point-to-point}}	Interface	Configures OSPF network type in OSPF interface.

10.2.3 OSPF Interface

OSPF configuration can be changed. Users are not required to alter all of these parameters, but some interface parameters must be consistent across all routers in an attached network.

10.2.3.1 Configuring Authentication

Authentication encodes communications among the routers. This function is for security of information in OSPF router.

Use the following command to configure authentication of OSPF router for security.

Command	Mode	Description
ip ospf authentication [message-digest null]	Interface	Enables Authentication on OSPF interface.
ip ospf A.B.C.D authentication [message-digest null]		



message-digest uses MD5 to encode for authentication, **null** means not using any of authentication.

Use the following command to release the configured authentication of OSPF router for security.

Command	Mode	Description
no ip ospf authentication [message-digest null]	Interface	Disables Authentication on OSPF interface.
no ip ospf A.B.C.D authentication [message-digest null]		

10.2.3.2 Configuring Authentication Key

If authentication enables on OSPF router interface, the password is needed for authentication. The authentication key works as a password. The authentication key must be consistent across all routers in an attached network.

Use the following command to configure the authentication-key which is based on text encoding.

Command	Mode	Description
ip ospf authentication-key {first second} active	Interface	Configures the authentication which is based on text encoding..
ip ospf authentication-key KEY {first second} [active]		
ip ospf authentication-key KEY A.B.C.D {first second}		
ip ospf authentication-key KEY A.B.C.D {first second} active		

Use the following command to configure the authentication which is based on md5 type.

Command	Mode	Description
ip ospf message-digest-key <1-255> md5 KEY active	Interface	Configures the authentication which is based on text encoding..
ip ospf message-digest-key <1-255> md5 KEY active		
ip ospf message-digest-key <1-255> md5 A.B.C.D active		
ip ospf message-digest-key <1-255> md5 active		

Clear Text Authentication.

1. Configure 2 keys, the first key and second.
2. The specified "active" key is used for encoding OSPF authentication in sender (OSPF router). If "active" doesn't exist, the first key will be used for encoding.
3. The specified "active" key is also used for OSPF authentication in receiver (OSPF router). If "active" doesn't exist, the first key will be used for encoding. But, if OSPF authentication fails using "active" key, the second key will be used for authentication.

MD5 Authentication.

- I. MD5 Authentication follows the way that ZebOS provides (1 through 255).
- II. The specified "active" key is used for encoding OSPF MD5 authentication in sender (OSPF router). If "active" key does not exist, it uses the last key in sorted order and encodes the key for authentication.
- III. Decoding will be done based on receiver's (OSPF router) key ID regardless of "active" state.

10.3 Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is commonly used, for use in small, homogeneous networks. It is a classical distance-vector routing protocol with using hop count. RIP is documented in RFC 1058. RIP uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. The OS software sends routing information updates every 30 seconds. This process is termed advertised. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the non-updating router as being unusable. If there is still no update after 120 seconds, the router removes all routing table entries for the non-updating router. The metric that RIP uses to rate the value of different routes is hop count. The hop count is the number of routers that can be traversed in a route. A directly connected network has a metric of zero; an unreachable network has a metric of 16. This small range of metrics makes RIP an unsuitable routing protocol for large networks. A router that is running RIP can receive a default network via an update from another router that is running RIP, or the router can source (generate) the default network itself with RIP. In both cases, the default network is advertised through RIP to other RIP neighbors. RIP sends updates to the interfaces in the specified networks.

If an interface's network is not specified, it will not be advertised in any RIP update. The system supports RIP version 1 and 2.

10.3.1 Enabling RIP

To use RIP protocol, you should enable RIP.

Step 1

To open *Router Configuration* mode, use the following command.

Command	Mode	Description
router rip	Global	Opens <i>Router Configuration</i> mode and operates RIP routing protocol.

Step 2

Configure network to operate as RIP.

Command	Mode	Description
network { <i>IP-ADDRESS</i> <i>INTER-FACE</i> }	Router	Configures network to operate as RIP.

The command **network** *IP-ADDRESS* enables RIP interfaces between certain numbers of a special network address. For example, if the network for 10.0.0.0/24 is RIP enabled, this would result in all the addresses from 10.0.0.0 to 10.0.0.255 being enabled for RIP. RIP packet is transmitted to port specified with the command, **network** *INTERFACE*.

- RIP Neighbor Router
- RIP Version
- Creating Static Route Available for RIP
- Transmitting Routing Information
- Metrics for Redistributed Routes

- Administrative Distance
- Creating Default Route
- Routing Information Filtering
- Routing Time
- Split-horizon
- Managing Authentication Key
- Monitoring and Managing RIP

10.3.2 RIP Neighbor Router

Since RIP is broadcast protocol, routers should be connected to transmit routing information of RIP to non-broadcast network.

To configure neighbor router to transmit RIP information, use the following command.

Command	Mode	Description
neighbor <i>IP-ADDRESS</i>	Router	Configures neighbor router to transmit routing information.



You can block routing information to specific interface by using `passive-interface` command.

10.3.3 RIP Version

Siemens' routers basically support RIP version 1 and 2. However, you can configure to receive only version 1 type packet or only version 2 type packet.

To configure RIP version, use the following command.

Command	Mode	Description
version {1 2}	Router	Configures version to transmit one of RIP 1 type packet and RIP 2 type packet.
no version {1 2}		Returns to default mode after specified RIP version is deleted.

The preceding task controls default RIP version settings. You can override the routers RIP version by configuring a particular interface to behave differently. To control which RIP version an interface sends, perform one of the following tasks after opening RIP *Router Configuration* mode.

Command	Mode	Description
ip rip send version 1	Interface	Sends RIP version 1 type packet to the interface.
ip rip send version 2		Sends RIP version 2 type packet to the interface.
ip rip send version 1 2		Sends RIP version 1 and 2 type packets.

Similarly, to control how packets received from an interface are processed, perform one of the following tasks.

Command	Mode	Description
ip rip receive version 1	Interface	Receives RIP version 1 type packet from the interface.
ip rip receive version 2		Receives RIP version 2 type packet from the interface.
ip rip receive version 1 2		Receives RIP version 1 and 2 type packets.

10.3.4 Creating Static Route Available for RIP

This feature is provided only by Siemens' route command creates static route available only for RIP. If you are not familiar with RIP protocol, you would better use redistribute static command.

Command	Mode	Description
route <i>IP-ADDRESS/M</i>	Router	Creates static route available only for RIP.

10.3.5 Transmitting Routing Information

The hiD 6610 S311 can redistribute routing information from a source route entry into the RIP tables. For example, you can instruct the router to re-advertise connected, kernel, or static routes as well as routing protocol-derived routes. This capability applies to all the IP-based routing protocols.

To redistribute routing information from a source route entry into the RIP table, use the following command.

Command	Mode	Description
redistribute { kernel connected static ospf bgp isis }	Router	Registers transmitted routing information in another router's RIP table.

You may also conditionally control the redistribution of routes between the two domains using **route map** command.

To define a route map for redistribution, use the following command.

Command	Mode	Description
route-map <i>WORD</i> { deny permit } <1-65535>	Global	Creates route map. 1-65535: sequence number
no route-map <i>WORD</i> { deny permit } <1-65535>		Deletes route map 1-65535: sequence number

One or more **match** and **set** commands typically follow **route-map** command. If there are no **match** commands, then everything matches. If there are no set commands, nothing is done. Therefore, you need at least one match or set command.

To define conditions for redistributing routes from a source route entry into the RIP tables, perform at least one of the following tasks in route-map configuration node.

Command	Mode	Description
match interface <i>INTERFACE</i>	Route-Map	Transmits information to only specified interface.
match ip address { <i>ACCESS-LIST-NAME</i> <i>PREFIX-LIST</i> <i>IP-ADDRESS</i> }		Transmits information matched with access-list or prefix-list.
match ip next-hop { <i>ACCESS-LIST-NAME</i> <i>PREFIX-LIST</i> <i>IP-ADDRESS</i> }		Transmits information to only neighbor router in access-list or prefix-list.
match metric <0-4294967295>		Transmits information matched with specified metric, enter the metric value.
ip next-hop <i>IP-ADDRESS</i>		Configures Neighbor router address.
metric <1-2147483647>		Configures metric value.

10.3.6 Metrics for Redistributed Routes

The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count and the OSPF metric is a combination of five quantities. In such situations, an artificial metric is assigned to the redistributed route. Because of this unavoidable tampering with dynamic information, carelessly exchanging routing information between different routing protocols can create routing loops, which can seriously degrade network operation.

To set metrics for redistributed routes, use the following command.

Command	Mode	Description
default-metric <i>VALUE</i>	Router	Configures same metric for all route transmitted by routing protocol, enter the value.



The metric of all protocol can be configured from 0 to 4,294,967,295. It can be configured from 1 to 16 for RIP.

10.3.7 Administrative Distance

Distance value represents confidence of routing information created by router. In large scaled network, some routing protocols or routing information may be more confident than other protocols or routers. Therefore, although a router has many routing protocols, the most confident route can receive routing information. When user configures distance value, router can find where routing information is created. Router always selects route created by routing protocol of the smallest distance value. Each network has its own features. So, there is no general rule for distance configuration. You should consider overall network to configure distance value.

To configure distance value, use the following command.

Command	Mode	Description
distance <1-255> [IP-ADDRESS/M [ACCESS-LIST-NAME]]	Router	Configures distance value.

10.3.8 Creating Default Route

You can force an autonomous system boundary router to generate a default route into an RIP routing domain. Whenever you specifically configure redistribution of routes into an RIP routing domain, the router automatically becomes an autonomous system boundary router. However, an autonomous system boundary router does not, by default, generate a default route into the RIP routing domain.

To force the autonomous system boundary router to generate a default route, use the following command.

Command	Mode	Description
default-information originate	Router	Forces the autonomous system boundary router to generate a default route into the RIP routing domain.

10.3.9 Routing Information Filtering

You can filter routing protocol information by performing the following tasks.

- Suppress sending of routing updates on a particular router interface. This is done to prevent other systems on an interface from learning about routes dynamically.
- Apply an offset to routing metrics. This is done to provide a local mechanism for increasing the value of routing metrics.

Blocking Outgoing Routing Information to Interface

To prevent other routers on a local network from learning about routes dynamically, you can keep routing update messages from being sent through a router interface. This feature applies to all IP-based routing protocols except BGP.

Command	Mode	Description
passive-interface INTERFACE	Router	Blocks routing information from interface of router.

Configuring Offset List

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. You can limit the offset list with an access list.

To increase the value of routing metrics, use the following command.

Command	Mode	Description
offset-list ACCESS-LIST-NAME {in out} <0-16> [INTERFACE]	Router	Applies an offset to routing metrics.

10.3.10 Routing Timer

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better you're your internet needs. The default settings for the timers are as follows.

- The update timer is 30 seconds. Every update timer seconds, the RIP process is awakened to send an unsolicited response message containing the complete routing table to all neighboring RIP routers.
- The timeout timer is 180 seconds. Upon expiration of the timeout, the route is no longer valid; however, it is retained in the routing table for a short time so that neighbors can be notified that the route has been dropped
- The garbage collect timer is 120 seconds. Upon expiration of the garbage-collection timer, the route is finally removed from the routing table.

To adjust the timers, use the following command.

Command	Mode	Description
timers basic <i>UPDATE TIMEOUT</i> <i>GARBAGE</i>	Router	Adjusts routing protocol timers.

10.3.11 Split-horizon

Normally, routers that are connected to broadcast-type IP networks and that use distance-vector routing protocols employ the split horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken. However, with non broadcast networks, such as Frame Relay, situations can arise for which this behavior is less than ideal. For these situations, you might want to disable split horizon.

If an interface is configured with secondary IP addresses and split horizon is enabled, updates might not be sourced by every secondary address. One routing update is sourced per network number unless split horizon is disabled.

To activate or deactivate or disable split horizon, perform the following tasks in interface configuration mode.

Command	Mode	Description
ip split-horizon	Interface	Activates Split horizon.
no ip split-horizon		Deactivates Split horizon.

10.3.12 Managing Authentication Key

RIP Version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, you can enable RIP authentication on an interface.

The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, plain text authentication can be performed using string command.

We support two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication. The default authentication in every RIP Version 2 packet is plain text authentication.



Do not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIP Version 2 packet. Use plain text authentication when security is not an issue, for example, to ensure that wrongly configured hosts do not participate in routing.

To configure RIP authentication, use the following command.

Command	Mode	Description
ip rip authentication <i>KEY-CHAIN NAME</i>	Interface	Activates RIP authentication.
ip rip authentication mode {text md5}		Configures the interface to use MD5 digest authentication or let it default to simple password authentication.
ip rip authentication string <i>STRING</i>		Configures the interface with plain text authentication. The string must be shorter than 16 characters.

10.3.13 Monitoring and Managing RIP

You can display specific router statistics such as the contents of IP routing tables, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also discover the routing path your router's packets are taking through the network.

To display various router statistics, use the following command.

Command	Mode	Description
show ip rip	Enable Global	Shows RIP information being used in router.
show ip route rip		Shows routing table information concerned with RIP.
show ip protocols [rip]		Shows current status of using RIP protocol and the information.

To quickly diagnose problems, the command debugging is meaningful and useful to customers.

To display information on RIP routing transactions, use the following command.

Command	Mode	Description
debug rip events	Enable Global	Shows RIP event such as packet transmit and sending and changed RIP information.
debug rip packet [recv send]		Shows more detail information about RIP packet. The information includes address of packet transmission and port number.
debug rip packet [recv send] detail		
show debugging rip		Shows all information configured for RIP debugging.

11 Abbreviations

ACL	Access Control List
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CBS	Committed Burst Size
CE	Communauté Européenne
CIDR	Classless Inter Domain Routing
CIR	Committed Information Rate
CLI	Command Line Interface
CoS	Class of Service
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check/Code
DA	Destination Address
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Service Code Point
EGP	Exterior Gateway Protocol
EMC	Electro-Magnetic Compatibility
EN	Europäische Norm (European Standard)
ERP	Ethernet Ring Protection
FDB	Filtering Data Base
FE	Fast Ethernet
FTP	File Transfer Protocol
GB	Gigabyte
GE	Gigabit Ethernet
hiD	Access Products in SURPASS Product Family
HW	Hardware
I ² C	Inter - Integrated Circuit interface
ID	Identifier
IEC	International Electro technical Commission
IEEE 802	Standards for Local and Metropolitan Area Networks
IEEE 802.1	Glossary, Network Management, MAC Bridges, and Internetworking

IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IRL	Input Rate Limiter
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunications standardization sector
L2	Layer 2
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LCT	Local Craft Terminal
LLC	Logical Link Control
LLDP	Link Layer Discover Protocol
LOF	Loss of Frame
LOL	Loss of Link
LOS	Loss of Signal
LPR	Loss of Power
MAC	Medium Access Control
NE	Network Element
OAM	Operation, Administration and Maintenance
ORL	Output Rate Limiter
OS	Operating System
OSPF	Open Shortest Path First
PC	Personal Computer
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
QoS	Quality of Service
RFC	Request for Comments
RIP	Routing Information Protocol
RSTP	Rapid Spanning Tree Protocol
RTC	Real Time Clock

SA	Source Address
SFP	Small Form Factor Pluggable
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
SW	Software
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TFTP	Trivial FTP
TMN	Telecommunication Management Network
TOS	Type of Service
UDP	User Datagram Protocol
UMN	User Manual
VID	VLAN ID
VLAN	Virtual Local Area Network
VoD	Video on Demand
VPI	Virtual Path Identifier
VPN	Virtual Private Network
xTU-C	xDSL Terminal Unit Central
xTU-R	xDSL Terminal Unit Remote